CITY OF REDLANDS

CITY COUNCIL

A G E N D A

October 6, 2026

MARIO SAUCEDO
Mayor
District 3

MARC SHAW
Mayor Pro Tempore
District 4

PAUL BARICH
Council Member
District 5

EDDIE TEJEDA
Council Member
District 2

DENISE DAVIS
Council Member
District 1

JEANNE DONALDSON
City Clerk

PHILLIP DOOLITTLE
City Treasurer

CHARLES M. DUGGAN JR.
City Manager

YVETTE M. ABICH GARCIA
City Attorney

5:00 p.m. Open Public Meeting, Public Comment (Closed Session)
6:00 p.m. Open Session (Public Meeting)
* * *
City Council Chambers
Civic Center, 35 Cajon Street, Suite 2, Redlands, California

A G E N D A

The following information comprises the agenda for the regular meeting of the City Council of the City of Redlands at the times noted below in the City Council Chambers, Civic Center, 35 Cajon Street, Suite 2, Redlands, California, on:

Tuesday, October 6, 2026

To join via Zoom on a computer, laptop, or smart device
Please visit www.zoom.us, click on Join a Meeting
Enter the **Meeting ID 896 2789 8341,** then run the Zoom launcher
To join via Zoom with audio only (cell phone or landline)
Dial **1-877-853-5247**
Enter the **Meeting ID 896 2789 8341**

Should the City lose connectivity on Zoom, we will halt the meeting until it can be restored. To check on the status of remote connectivity in the event of an outage, go to the City's website at www.cityofredlands.org or to the City's Facebook page at @CityofRedlands or the Instagram page at @CityofRedlands_CityHall.

In the event the City cannot reestablish Zoom connectivity in a reasonable amount of time, the Mayor will adjourn the meeting to a future date.

PLEASE NOTE: Anyone desiring to speak on an agendized item at this meeting may do so during the consideration of that time. Due to time constraints and the number of persons who may wish to give oral testimony, public comments will be limited to three (3) minutes.

- **To provide comment while participating from Council Chambers:**
  - Although it is not required, speakers are encouraged to submit a "Speaker Sign Up Sheet" before the meeting is convened. Forms are available in the Office of the City Clerk or in Council Chambers.
  - After the meeting has convened, you may place the speaker form in the basket at the table along the north wall of the Chambers. Please do not disturb the City Clerk while the meeting is in progress.
- **To provide comment through Zoom (on a computer, laptop, or smart device)**
  - Click the "Raise Hand" button and the moderator will unmute you when it is your turn to speak
- **To provide comment via audio only (cell phone or landline)**
  - Dial *9 to "Raise Hand". The moderator will identity you by your area code and last 3 numbers of your telephone number when it is your turn to speak.

PLEASE SILENCE CELL PHONES, PAGERS AND OTHER ELECTRONIC COMMUNICATION DEVICES UPON ENTERING THE CHAMBERS

5:00 PM

A. Call City Council Meeting to Order

B. Public Comment

(Any person wishing to provide public comment on a closed session matter may do so at this time.)

C. Recess City Council Meeting to a Closed Session

1. Performance Evaluations of Public Employees – Government Code § 54957(b)(1)
   Positions: City Manager and City Attorney

2. Conference with Labor Negotiator - Government Code § 54957.6
   Agency Negotiators: Mayor Saucedo and Mayor Pro Tem Shaw
   Unrepresented Employees: City Manager and City Attorney

3. Conference with real property negotiators - Government Code § 54956.8
   (Tabitha Crocker, Facilities and Community Services Director)

   Property: APN 0171-089-13-0000
   Agency Negotiators: Charles M. Duggan, Jr., City Manager; Tabitha Crocker, Facilities and Community Services Director
   Negotiating Party: Zachary D. Smith
   Under Negotiation: Price and terms of payment for possible purchase of property

D. Reconvene City Council Meeting at 6:00 p.m.

E. Invocation by Council Member Davis - Pledge of Allegiance by Arroyo Verde Elementary School

(In keeping with long-standing traditions of legislative invocations, this City Council meeting may include a brief invocation. Such invocations are not intended to proselytize or advance any one, or to disparage any other, faith or belief. Neither the City nor the City Council endorses any particular religious belief or form of invocation.)

F. Closed Session Report

(No reportable action taken in closed session unless otherwise announced by the City Attorney at this time.)

G. Presentations

1. Redlands Pet Adoption
   (Redlands Animal Services)

2. Presentation of the Hindu Heritage Month Proclamation presented to Roop Kishor Goyal
   (Mayor Saucedo)

H. Public Comment - City Council

I. Consent Calendar

(The following routine items have been recommended for approval and will be acted upon simultaneously unless separate discussion and/or action is requested by a Councilmember or a member of the audience.)

1. Approval of minutes of the regular meeting of September 15, 2026
   (City Clerk Donaldson)

2. Approval of minutes of the special meeting of September 21, 2026
   (City Clerk Donaldson)

3. Authorize the issuance of a Proclamation declaring the month of October 2026 Hindu Heritage Month in the City of Redlands
   (Mayor Saucedo)

4. Approve an Intergovernmental Purchase of Palo Alto Networks Firewall Software Support for One Year from Sidepath, Inc. in the amount of $100,100
   (Assistant City Manager Garcia)

5. Approve an Assignment of Trademark and Domain Name with the Redlands Historical Museum Association and determine that approval is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines
   (Assistant City Manager Garcia)

6. Authorize the Annual Maintenance Payment to Motorola Solutions, Inc. in the amount of $126,956 for the Police Department's Spillman Computer Aided Dispatch/Records Management System
   (Assistant City Manager Garcia)

7. Approve an Intergovernmental Purchase of Dell Computers and Accessories for a Citywide Computer Refresh in the amount of $130,206
   (Assistant City Manager Garcia)

8. Approve Final Map for Tract No. 20402 prepared and submitted by TH Canyon Ranch Loma Linda LLC located at the northeast corner of Nevada Street and San Timoteo Canyon Road and approximately 400 feet south of Bermudez Street
   (Development Services Director Reilly)

9. Approve an Agreement with TH Canyon Ranch Loma Linda, LLC regarding operation and maintenance of a private lift station and force main serving Tract No. 20402 in San Timoteo Canyon and determine that the approval of the proposed agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's guidelines implementing the California Environmental Quality Act
   (Development Services Director Reilly)

10. Adopt Resolution No. 8827 adopting the 2026 City of Redlands Emergency Operations Plan
    (Fire Chief Sessler)

11. Approve the side letter agreement between the City of Redlands and Redlands Police Officers Association (RPOA), which amends and modifies Article 8 of the RPOA Memorandum of Understanding (MOU) pertaining to Field Training Officer Sergeant Incentive Pay
(Human Resources/Risk Management Director King)

12. Approve a Fourth Amendment to the Professional Services Agreement with Carollo Engineers, Inc. for the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project extending the completion time to December 31, 2028
(Municipal Utilities and Engineering Director Heredia)

13. Approve a Professional Services Agreement with Biggs Cardosa Associates, Inc. for conceptual engineering design of the Citrus Avenue and Redlands High School Crossing Project for an amount not to exceed $216,482; approve a Cooperative Agreement with Redlands Unified School District; re-designate a portion of the current $1,500,000 budgeted in the Arterial Street Fund 252 to the Local Transportation Fund 209 and Measure I Fund 210; and determine that approval of these agreements is not subject to environmental review under Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act
(Municipal Utilities and Engineering Director Heredia)

14. Approve the Interlocal Agreement between the Town of Apple Valley and the Cities of Adelanto, Barstow, Chino, Colton, Fontana, Hesperia, Highland, Montclair, Ontario, Rancho Cucamonga, Redlands, Rialto, San Bernardino, Upland, Victorville, Yucaipa and San Bernardino County for the 2025 Justice Assistance Grant Award and approve an additional appropriation of $16,248 to the Redlands Police Department
(Police Chief Tolber)

15. Approve the use of City resources and an in-kind request in the amount of $5,798.32 related to A Holiday Evening with Phat Cat Swinger event held on Friday, December 4, 2026, hosted by Redlands Bowl Performing Arts; approve various temporary street closures; and determine that the event is categorically exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act
(Facilities and Community Services Director Crocker)

16. Approve the use of City resources and an in-kind request in the amount of $17,922.00 related to the Redlands Turkey Trot event held on Thursday, November 26, 2026, hosted by Phoenix Hope International; approve various temporary street closures; and determine that the event is categorically exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act
(Facilities and Community Services Director Crocker)

17. Authorize the sale and consumption of alcoholic beverages and temporary street closures related to the REVEL Big Bear Marathon event held on Saturday, November 7, 2026, by the Brooksee Foundation and determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act
(Facilities and Community Services Director Crocker)

18. Adopt Resolution No. 8835, Rescinding Resolution No. 8809, Reaffirming the levying of special taxes within the City of Redlands Community Facilities District No. 2004-1, and directing the San Bernardino County Auditor/Controller/Treasurer/Tax Collector to place the City of Redlands Community Facilities District No. 2004-1 Special Taxes on the Fiscal Year 2026-2027 Tax Roll
(Facilities and Community Services Director Crocker)

J. Communications

1. Conference Report- 2026 League of California Cities Annual Conference and Expo
(Mayor Saucedo, Mayor Pro Tem Shaw and Council Member Davis)

2. Adopt Resolution No. 8834 supporting Proposition 1, the Veterans and Affordable Housing Bond Act of 2026, which authorizes $11.25 billion in state general obligation bonds to fund several housing affordability programs
(Mayor Saucedo)

3. Discussion and possible action to approve Resolution No. 8837 amending the procedures and guidelines for reviewing applications to fill vacancies on the Planning Commission and rescinding Resolution No. 8674
(Mayor Pro Tem Shaw)

4. Discussion and possible action relating to the formation of, and appointments to, an Ad Hoc Committee of the City Council to review applications for vacancies of the Planning Commission
(Mayor Saucedo)

K. Public Hearings

1. CONTINUED PUBLIC HEARING to consider Ordinance Text Amendment No. 372 to amend Title 18 (Zoning Regulations) of the Redlands Municipal Code to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses; consideration of a proposed amendment to Chapter 18.156, Article XII (Warehouses and Logistics Distribution Centers) to add new Section 18.156.970 for new rebuilding provisions for existing warehouses and logistics distribution centers; and consideration of Resolution No. 8793 to amend the commercial and industrial Specific Plans of the City of Redlands to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses. The proposal qualifies for exemption from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines
(Development Services Director Reilly)

L. New Business

1. Approve the First Amendment to the Public Works Contract with B-81 Paving Inc. for On-Call Pavement Repair Services for Water Utilities to increase the not to exceed amount from $600,000 to $900,000
(Municipal Utilities and Engineering Director Heredia)

2. Consideration of an agreement with Three Peaks Corp. for the crushing of concrete stockpile for a three-year term in a total amount not to exceed $300,000 and determination that the project is exempt from environmental review pursuant to Section 15301 of the State's Guidelines implementing the California Environmental Quality Act

   (Facilities and Community Services Director Crocker)

3. Consideration of a Purchase and Sales Agreement with Zachary D. Smith, an individual, for the property located at 21 N. Church Street (Assessor Parcel Number 0171-089-13-0000), and determine that the approval of the Agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act

   (Facilities and Community Services Director Crocker)

M. Individual Council Member Announcements and/or Reports on Activities

(No collective discussion or action.)

1. Individual Council Member Report on Activities for September 2026 from Mayor Pro Tem Shaw

   Mayor Pro Tem Shaw has requested to include this report on the agenda for recording purposes. The report does not require City Council approval.

N. Adjournment

If you challenge any proposed development entitlement listed on this agenda in court, you may be limited to raising only those issues you or someone else raised at the public hearing described in this notice, or in written correspondence delivered to the City Council at or prior to this public meeting.

In compliance with the Americans with Disabilities Act, if you need special assistance to participate in this meeting, please contact Goutam Dobey, of the Municipal Utilities and Engineering Department at (909) 798-7584 ext 2. Notification 48 hours prior to the meeting will enable the City to make reasonable arrangements to ensure accessibility to this meeting.

(28 CFR 35.102-35.104 ADA Title II)

Any writings or documents distributed to a majority of the City Council Regarding an open session agenda item less than 72 hours before this meeting are available for public inspection at the City Clerk's Office or at the dais of the City Clerk once the open session begins.

Staff reports or other written documentation relating to items referred to on the agenda are available at the A. K. Smiley Public Library, 125 West Vine Street, Redlands, California, and on the City's Website referenced below.

Regular meetings are televised live on Redlands TV Channel 3 (Spectrum) and Channel 35 (Frontier) and re-broadcast at 7:00 P.M. The following Wednesday, Friday and Sunday; and at 9:00 A.M. Thursday, Saturday, and Monday. Meetings are also streamed live and archived for later viewing on demand on the City's website at www.cityofredlands.org. Agendas, staff reports and minutes of the City Council of the City of Redlands are available online at: www.cityofredlands.org

Date Posted: October 1, 2026

City Council **AGENDA ITEM NO. I1.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approval of minutes of the regular meeting of September 15, 2026 (City Clerk Donaldson)

MOTION:

I move to approve the regular meeting minutes of September 15, 2026.

Attachments

City Council-09-15-2026-minutesDraft.pdf

MINUTES

Regular meeting of the City Council of the City of Redlands held in the Council Chambers, Civic Center, 35 Cajon Street, on Tuesday, September 15, 2026 at 5:00 P.M.

Present:	Mario Saucedo, Mayor Marc Shaw, Mayor Pro Tempore Paul Barich, Council Member Eddie Tejeda, Council Member Denise Davis, Council Member
Staff:	Charles M. Duggan, Jr., City Manager; Yvette M. Abich Garcia, City Attorney; Jeanne Donaldson, City Clerk; Phillip Doolittle, City Treasurer; Danielle Garcia, Assistant City Manager; Kurt O. Wilson, Assistant City Manager; Carl Baker, Public Information Officer; Rich Sessler, Fire Chief; Jeremy Floyd, Deputy Police Chief; Tabitha Crocker, Facilities and Community Services Director; Monica Heredia, Municipal Utilities and Engineering Director; Gina King, Human Resources/Risk Management Director; James Garland, Finance Director

A. Call City Council Meeting to Order

B. Public Comment

There was no public comment.

C. Recess City Council Meeting to a Closed Session

1. Conference with legal counsel: Existing Litigation - Government Code § 54956.9(d)(1)

Three Cases:

a. Coyote Aviation, Inc. v. City of Redlands, et al. San Bernardino County Superior Court Case No. CIVSB2418252

b. Simpson v. City of Redlands, San Bernardino Superior Court, Case No. CIVSB2435099

c. Orozco v. City of Redlands, San Bernardino Superior Court, Case No. CIVSB2527564

D. Reconvene City Council Meeting at 6:00 p.m.

Mayor Saucedo reconvened the Regular Meeting of the Redlands City Council and called to order the Special Meeting of the Redlands Housing Corporation. He recessed the Special Meeting of the Redlands Housing Corporation. The Housing Corporation will reconvene immediately following the conclusion of the Redlands City Council meeting.

E. Invocation by Council Member Tejeda - Pledge of Allegiance by eAcademy/RISE Elementary

F. Closed Session Report

City Attorney Garcia announced there was no reportable action taken in Closed Session.

G. Presentations

1. Presentation of the Hispanic Heritage Month Proclamation to Lucille Saldaña

Mayor Saucedo presented the Hispanic Heritage Month Proclamation to Lucille Saldaña.

2. Presentation of the California Native American Day Proclamation to Venessa Brierty, District Director, State Assemblymember James Ramos' Office

Mayor Saucedo presented the California Native American Day Proclamation to State Assemblymember James Ramos.

3. Presentation of the University of Redlands Softball Championship Proclamation presented to the University of Redlands Softball Team and Coaching Staff

Council Member Davis presented the Softball Championship Proclamation to the University of Redlands Softball Team and Coaching Staff.

4. Presentation of Montessori in Redlands 50th Anniversary Proclamation presented to Jenny Davidson, Head of School, Montessori in Redlands

Council Member Davis presented the Proclamation honoring Montessori's 50th anniversary in Redlands to Jenny Davidson, Head of School.

H. Public Comment - City Council

There was no public comment.

I. Consent Calendar

1. Approve minutes of the regular meeting of September 1, 2026

    On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, the minutes of the regular meeting of September 1, 2026.

    Vote: 5-0 Passed

2. Authorize issuance of a proclamation declaring September 15 through October 15, 2026, as Hispanic Heritage Month

    On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council authorized, by roll call vote, the issuance of a proclamation declaring September 15 through October 15, 2026 as Hispanic Heritage Month in the City of Redlands.

    Vote: 5-0 Passed

3. Authorize issuance of a proclamation declaring September 25, 2026, as California Native American Day

    On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council authorized, by roll call vote, the issuance of a proclamation declaring September 25, 2026 as California Native American Day in the City of Redlands.

    Vote: 5-0 Passed

4. Authorize issuance of a proclamation to the University of Redlands Women's Softball Team

    On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council authorized, by roll call vote, the issuance of a proclamation to the University of Redlands Women’s Softball Team

    Vote: 5-0 Passed

5. Authorize issuance of a proclamation celebrating Montessori in Redlands' 50th Anniversary

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council authorized, by roll call vote, the issuance of a proclamation celebrating Montessori in Redlands' 50th Anniversary.

Vote: 5-0 Passed

6. Disclosure of Settlement and Release Agreement – Armstrong Cal Builders, Inc. v. City of Redlands

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council disclosed, by roll call vote, the Settlement Agreement and Release between the City of Redlands and Armstrong Cal Builders, Inc. Under the terms of the agreement the City agrees to pay Armstrong Cal Builders, Inc a total of $108,698.49 to settle and dispose of disputes associated with civil action in the San Bernardino Superior Court , Case No. CIVSB2505450.

Vote: 5-0 Passed

7. Adopt Resolution No. 8832 rescinding Resolution No. 8663 and adopting a revised City Council Recognition Policy

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, Resolution No. 8832 rescinding Resolution No. 8663, adopting a revised City Council Recognition Policy to revise the proclamation request deadline from five weeks to three weeks prior to the scheduled City Council meeting.

Vote: 5-0 Passed

8. Approve a Memorandum of Understanding with University of Redlands for Paramedic Standby Services

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, the Memorandum of Understanding with the University of Redlands for standby paramedic services during university football games and other special events as needed.

Vote: 5-0 Passed

9. Approve the First Amendment to Agreement between Consolidated Fire Agencies (CONFIRE) and the City of Redlands for Ground Ambulance Transport Services

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, the First Amendment to the Agreement between the City of Redlands and Consolidated Fire Agencies (CONFIRE) for the provision of Ground Ambulance Transport Services.

Vote: 5-0 Passed

10. Adopt Resolution No. 8828 amending the City's Conflict of Interest Code to include new designated positions and remove positions that no longer make or participate in governmental decisions, acknowledge the City Council's review of the Conflict of Interest Code, and rescind Resolution No. 8628

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council adopted, by roll call vote, Resolution No. 8828 and acknowledged that this City Council has reviewed its Conflict of Interest Code and finds that the following amendments are necessary: (1) Include new positions that must be designated and (2) Delete positions that no longer make or participate in governmental decisions and rescinded Resolution No. 8628.

Vote: 5-0 Passed

11. Approve a purchase order with Evantec Corporation in the amount of $83,000 for joint utility laboratory supplies and determine that this action is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines

implementing the California Environmental Quality Act

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council determined, by roll call vote, that the approval of a purchase order with Evantec Corporation is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act; and approved a purchase order with Evantec Corporation in the amount of $83,000.

Vote: 5-0 Passed

12. Approve a Grant Agreement with the Office of Traffic Safety relating to the distribution of a grant award in an amount not to exceed $94,300 and authorize the Chief of Police to sign and execute the grant agreement; and approve an additional appropriation of the same amount

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, a Grant Agreement with the Office of Traffic Safety relating to the distribution of a grant award in an amount not to exceed $94,300; authorized the Chief of Police to sign and execute agreements implementing the grant; and approved an additional appropriation in the amount of $94,300.

Vote: 5-0 Passed

13. Approve an agreement with the California Department of Alcoholic Beverage Control for the Alcohol Policing Partnership Program Grant, approve an additional appropriation of $27,000 in grant funds to the Police Department, and authorize the Chief of Police to execute the agreement and related documents

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council approved, by roll call vote, the agreement between the City and the Department of Alcoholic Beverage Control (ABC) for the grant provided by the Alcohol Policing Partnership (APP) Program; approved the additional appropriation of $27,000 in grant funds to the Police Department; and authorized the Chief of Police to execute any necessary agreements related to the grant.

Vote: 5-0 Passed

14. Accept the 2026-2027 Community Development Block Grant (CDBG) funding award in the amount of $200,201 from the County of San Bernardino, approve an additional appropriation of the same, and adopt Resolution No. 8831 authorizing the City Manager, or designee, to execute the Grant Agreement and all other related documents

On motion of Council Member Paul Barich, seconded by Council Member Eddie Tejeda, the City Council accepted, by roll call vote, the 2026-2027 Community Development Block Grant (CDBG) program year funding award in the amount of $200,201; authorized an additional appropriation of $200,201 for the 2026-2027 Fiscal Year; and adopted Resolution No. 8831 authorizing the City Manager, or designee, to execute agreements, amendments and other related documents associated with the 2026-2027 CDBG Program Year.

Vote: 5-0 Passed

J. New Business

1. Consideration of Resolution No. 8833 Naming the Plaza at the New City Hall in Honor of Former City Attorney Dan McHugh

Council Member Barich suggested the City Council consider adopting Resolution No. 8833 naming the plaza located on the north side of the new City Hall at 300 E. State Street as "Dan McHugh Plaza," in recognition of former City Attorney Dan McHugh's longstanding service and contributions to the City of Redlands. Mr. McHugh served the City for approximately 35 years, including 28 years as City Attorney from 1994 until his retirement in 2022. During his tenure, he advised 18 City Councils and provided legal guidance on significant matters affecting the City. His

extensive institutional knowledge, dedication to public service, and lasting contributions to the Redlands community were highlighted by all the Council Members.

On motion of Council Member Paul Barich, seconded by Mayor Mario Saucedo, the City Council waived, by roll call vote, the three-year requirement established by Resolution No. 7711; and adopted Resolution No. 8833 naming the plaza located on the north side of the new City Hall at 300 E. State Street as “Dan McHugh Plaza.”

Vote: 5-0 Passed

2. Consideration of a Funding Agreement with Redlands Housing Corporation providing a $1,650,000 nonrepayable capital contribution toward acquisition of 1675 Industrial Park Avenue for permanent supportive housing, determine that approval of the agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines, and authorize a related additional appropriation

Assistant City Manager Garcia summarized a Funding Agreement with Redlands Housing Corporation providing a $700,000 non-repayable capital contribution toward acquisition of 1675 Industrial Park Avenue for permanent supportive housing and a related additional appropriation. Following Shangri-La Industries, LLC’s default and the subsequent foreclosure of the Homekey permanent supportive housing property at 1675 Industrial Park Avenue, the City and current owner have worked to maintain uninterrupted operations while pursuing a long-term ownership solution. The City formed the Redlands Housing Corporation as a nonprofit public benefit corporation and City instrumentality to acquire, own, govern, and operate the property consistent with its public purpose and applicable funding and regulatory requirements.

The proposed Funding Agreement documents the City's $1,650,000 non-repayable capital contribution toward the acquisition and closing of the property. The City's contribution is allocated as follows: $700,000 toward the purchase price, $600,000 toward payment of delinquent property taxes, $135,000 toward estimated Closing costs, $200,000 as a contingency for currently unknown costs that may arise before Closing, and $15,000 toward due diligence reports. Redlands Housing Corporation is intended to provide a separate nonprofit ownership structure that facilitates the continued operation of the Homekey property over the next several years and to serve as an interim owner until the property can be transferred in the coming years, subject to applicable State approvals and funding requirements, to an external, independent nonprofit organization for long-term operation as permanent supportive housing.

As public comment, Dennis Bell expressed concerns that funding could dry up, turning the project into a financial burden. Additionally, he questioned the property's valuation and the County Assessor's official assessment. As a way to increase the number of beds, he suggested the Council consider converting a few floors of the new city hall be dedicated to homeless housing.

On motion of Council Member Eddie Tejeda, seconded by Council Member Paul Barich, the City Council approved, by roll call vote, the Funding Agreement with Redlands Housing Corporation providing a $700,000 non-repayable capital contribution toward acquisition of 1675 Industrial Park Avenue for permanent supportive housing; determined that approval of the agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines, and authorize a related additional appropriation; authorized the City Manager to execute the Funding Agreement; and approved additional appropriation of $700,000 in the Homeless Solutions Budget for deposit into escrow in accordance with the Funding Agreement.

Vote: 5-0 Passed

3. Consideration of a National Pollutant Discharge Elimination System (NPDES) Stormwater Permit Implementation Agreement for the Santa Ana Region, NPDES NO. CAS618036, Order No. R8-2010-0036 establishing the responsibilities with respect to compliance with NPDES Stormwater regulations and sharing costs associated with the order in the amount of $139,323

Municipal Utilities and Engineering Director Heredia presented the need for the National Pollutant Discharge Elimination System (NPDES) Stormwater Permit Implementation Agreement, California Regional Water Quality

Control Board (SARWQCB), Santa Ana Region NPDES NO. CAS618036, Order No. R8-2010-0036 establishing the responsibilities with respect to compliance with NPDES Stormwater regulations and sharing costs associated with the Order $139,323 annually.

California administers the NPDES program through nine regional water quality control boards, with Redlands located in Region Eight, the Santa Ana Region. An Implementation Agreement sets the structure for coordinated permit administration, compliance responsibilities, and cost-sharing among participating agencies. The agreement ends when a new approved agreement takes effect. Under this arrangement, the City must contribute 5.25% of the total program cost annually, beginning in FY 2026/27, totaling $139,323. Mayor Saucedo asked whether the City's contribution amount will increase with the recent approval of a new permit by SARWQCB. Director Heredia clarified that during the SARWQCB meeting held September 11, 2026, a new permit was adopted, but at this time, it is unclear whether any additional contributions will be required of the City. An upcoming workshop scheduled for September 23 will provide more clarity.

On motion of Council Member Eddie Tejeda, seconded by Mayor Mario Saucedo, the City Council approved, by roll call vote, the Implementation Agreement for the National Pollutant Discharge Elimination System (NPDES) Stormwater Permit in compliance with the Santa Ana Region, NPDES No. CAS618036, Order No. R8-2010-0036.

Vote: 5-0 Passed

4. Consideration of a Professional Services Agreements with Hicks & Hartwick, Inc. to provide on-call general engineering services in an amount not to exceed $200,000 for the initial one-year term, with options to extend for one additional year for an amount not to exceed $200,000, for a total potential not to exceed value of $400,000; and determine that approval of the Agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act

Municipal Utilities and Engineering Director Heredia introduced a Professional Services Agreements with Hicks & Hartwick, Inc. to provide on-call general engineering services. The Agreement provides for the issuance of project-specific Task Orders which will define the project scope, required services, deliverables, schedule, and other applicable project requirements. Council Member Barich was pleased the engineering firm is local.

On motion of Council Member Paul Barich, seconded by Council Member Denise Davis, the City Council approved, by roll call vote, a Professional Services Agreement with Hicks & Hartwick, Inc. to provide on-call general engineering services in an amount not to exceed $200,000 for the initial one-year term, with an option to extend for one additional year in an amount not to exceed $200,000, for a total potential not to exceed value of $400,000; and determined that approval of the Agreement with Hicks & Hartwick, Inc. is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act.

Vote: 5-0 Passed

K. Individual Council Member Announcements and/or Reports on Activities

Mayor Saucedo attended the SBCTA meeting, a planning session for the Hispanic Heritage Month event, the Library Board meeting, and met with residents to discuss their concerns regarding property in San Timoteo Canyon.

Council Member Barich enjoyed some vacation time.

Council Member Tejeda attended the Parks and Recreation Committee meeting.

Council Member Davis toured the Feeding America warehouse in Riverside, and while there, also met with staff from the local Boys and Girls Club to review food security initiatives and the City's Food Security Task Force.

L. Adjournment

With no further action, the meeting adjourned at 6:44 p.m. The next regular meeting of the City of Redlands City Council will be held on October 6, 2026.

City Council **AGENDA ITEM NO. I2.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approval of minutes of the special meeting of September 21, 2026 (City Clerk Donaldson)

MOTION:

I move to approve the special meeting minutes of September 21, 2026.

Attachments

City Council-09-21-2026-minutesDraft.pdf

MINUTES

Special meeting of the City Council of the City of Redlands held in the Council Chambers, Civic Center, 35 Cajon Street, on Monday, September 21, 2026 at 5:00 P.M.

Present:	Mario Saucedo, Mayor Marc Shaw, Mayor Pro Tempore Paul Barich, Council Member Denise Davis, Council Member
	Absent: Eddie Tejeda, Council Member
Staff:	Charles M. Duggan, Jr., City Manager; Yvette M. Abich Garcia, City Attorney; Jeanne Donaldson, City Clerk; Phillip Doolittle, City Treasurer; Danielle Garcia, Assistant City Manager; Kurt O. Wilson, Assistant City Manager; Carl Baker, Public Information Officer; Rich Sessler, Fire Chief; Rachel Tolber, Police Chief; Tabitha Crocker, Facilities and Community Services Director; Sean Reilly, Development Services Director; Monica Heredia, Municipal Utilities and Engineering Director; Gina King, Human Resources/Risk Management Director; James Garland, Finance Director

A. Call City Council Special Meeting to Order

Mayor Saucedo called the special meeting to order at 5:00 p.m.

B. Public Comment

Logistics Facilities & Sustainability - John James argued that banning warehouse & logistics facilities is in direct opposition to the goals of the City's Climate Action Plan (CAP). He said the CAP focuses on moving people more efficiently to reduce emissions and traffic, just as logistics facilities strive to solve the identical problem of moving goods more efficiently to the consumer. Furthermore, prohibiting warehouses and the modernization of such facilities does not stop consumer demand or eliminate freight. Instead, it pushes warehouses out of town and shifts the environmental burden elsewhere while inflating costs and shipping emissions.

C. Communications

1. Discussion and Possible Action regarding the FY2027 and FY2028 Budget Update

    City Manager Duggan provided a budget update on the Adopted Biennial Budget for FY 2027 and 2028. The presentation recapped the General Fund budget, highlighted key budget reductions and revisions required to develop the adopted budget, reviewed recommended revisions made after adoption, including additional costs resulting from MOU negotiations and subsequent reductions, and outlined the next steps in the budget process for fiscal year 2027 and beyond.

    Revisions and Reductions:

    - $495,000 Elimination of Contract Code Enforcement
    - $1,200,000 Reduction of Tree Trimming Contract
    - $300,000 Elimination of Potential Ballot Measures
    - $550,000 Reduction of Fire Department Overtime
    - $439,000 Reduction in Police Department Overtime

- $817,000 Reduction in FCS and Fire Department Services and Supplies

Recommended Budget Revisions after adoption:

- $55,803 Elimination of 3 Part-Time Positions (1 Library, 2 Development Services)
- $50,000 Additional Reduction of Tree Trimming Contract
- $166,000 Additional Reduction of Police Department Overtime
- $143,000 Additional Reduction of Fire Department Overtime
- $90,000 Reduction in Material and Supplies (Multiple Departments)
- $420,000 Reduction in Services (Multiple Departments)
- $160,000 Reduction in IT Charges to PD and Fire (Absorbed in IT Budget)

Next Steps for FY 2027 and 2028

City Manager Duggan presented the City's long-term financial planning needs for FY27 and FY28, with projections extending through FY32. He focused on the desire to develop a sustainable approach to anticipated financial challenges, such as the planned $4.5 million in budget reductions beginning in FY29. He offered an overview of Measure T spending for FY 27 and FY 28 and responded to several Council Member questions. In conclusion, he reviewed the budget calendar.

As public comment, Dennis Bell said the City was its own worst enemy and has historically struggled to make tough decisions. He voiced concerns about cutting police and fire overtime hours. Council Members expressed their appreciation of staff's thorough reporting while City Manager Duggan thanked Finance Director James Garland and his team for preparing the update.

2. Discussion and Possible Action of a Fee Schedule for City Services provided in support of eligible nonprofit events pursuant to Resolution No. 8780

Facilities and Community Services Department Director Crocker introduced a fee schedule regarding estimated costs for city services provided in support of eligible nonprofit events pursuant to Resolution No. 8780. In 2021, the City Council adopted Resolution No. 8220 establishing a formal policy for evaluating requests from nonprofit organizations seeking in-kind support through the contribution of city resources for special events.

In support of these events, the City has absorbed the costs associated with providing in-kind support through existing departmental operating budgets. These costs include personnel time, Public Safety staffing and resources, Public Works services, facility and park use, traffic control, equipment, permit administration, and other municipal resources.

Resolution No. 8780, approved in April 2026, established a defined list of historically supported nonprofit events that are eligible to continue receiving in-kind city services. During the adoption of Resolution No. 8780, the City Council also directed staff to return with a fee schedule identifying the estimated value of city services provided for the eligible events. Director Crocker listed fees that currently exist and may be applied to recover costs associated with various in-kind events and provided three examples illustrating how fees could be applied.

As public comment, Andy Hoder was pleased the City was considering sharing event costs with nonprofit organizers, and he suggested fees could be split 50/50. Dennis Bell cited the Redlands Bicycle Classic as another instance of the City's overly generous in-kind support.

Council Members raised several questions related to the implementation of the fees and how best to apply fees equitably. Director Crocker confirmed that all special events will undergo individual review and discussion at City Council Meetings, with any applicable fees determined at that time. City Manager Duggan added that charges for City services will continue to grow due to the increase in labor costs. Mayor Saucedo urged his colleagues to prepare for difficult decisions to curb spending and ensure fiscal responsibility.

3. Discussion and Possible Action regarding the 7th & 9th Street Parking Lot and other parking related projects in the Downtown area

Economic Development Coordinator Ross Wittman provided background on the discussion regarding the 7th & 9th Street Parking Lot and downtown parking needs and explained this was a follow up to previous City Council discussions related to parking. The downtown area has become a vibrant regional destination drawing large crowds to the area. The crowds support the local economy but also place demands on the parking infrastructure.

The City has evaluated the scarcity of downtown parking, funded additional short and long-term parking solutions, and started exploring ways to increase parking supply. This includes a temporary lease at the Mall site of approximately 500 spaces at an annual cost of approximately $350,000. It also includes two scenarios at 35 Cajon St. The first would create 279 spaces for approximately $4 million. The second would create 547 spaces + 10,000 sf of retail space for approximately $28 million. Fully evaluating these options would require the prioritization of staffing resources and implementing them would require additional funding.

The San Bernardino County Transportation Commission (SBCTA) owns a vacant parcel of land North of Redlands Blvd between 7th and 9th Streets immediately south of the railroad tracks. With a capital investment, the two-acre site could accommodate approximately 140 parking spaces within a short walk of State Street but requires crossing Redlands Blvd.

Conversations with SBCTA indicate the lot could be leased for a nominal annual cost but would require approximately $750,000 in capital investments. A recent appraisal of the property places the value at approximately $1.15 million. SBCTA has indicated they may be willing to sell the property. Mr. Wittman summarized the options to lease and/or to purchase the property. Each of the options has the potential to expand downtown parking supply but the associated costs are considerable.

Council Members Barich and Davis insisted the project would waste time and capital, claiming the public simply would not park that far from downtown. As public comment, Dennis Bell agreed that people would refuse to park at the SBCTA site, just as the public already routinely avoids parking at Centennial Plaza. With the closing of Look Theater, he suggested the City consider purchasing their parking lot. Andy Hoder advised the Council against adopting the paid parking models of other cities, encouraging instead the continuation of free parking.

Council Members agreed that due to the City's current budget constraints, moving forward with any options as presented was not feasible, and they directed staff to notify the appropriate entities that the City does not intend to pursue the 7th and 9th Street lot or any of the parking-related options at this time.

D. Adjournment

With no further action, the special meeting adjourned at 6:03 p.m.

City Council **AGENDA ITEM NO. I3.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Authorize the issuance of a Proclamation declaring the month of October 2026 Hindu Heritage Month in the City of Redlands (Mayor Saucedo)

MOTION:

I move to authorize the issuance of a Proclamation declaring the month of October 2026 Hindu Heritage Month in the City of Redlands.

Attachments

Hindu Heritage Month 2026.pdf

PROCLAMATION

Hindu Heritage Month

WHEREAS, there are an estimated one billion Hindus worldwide and approximately four million Hindu Americans in the United States; and

WHEREAS, the City of Redlands is home to a large and growing population of Hindu Americans; and

WHEREAS, the practice of Hinduism seeks to promote unity among all Dharmic and other communities, increase awareness of Hindu values and educate society on issues affecting the Hindu American community; and

WHEREAS, Hindu Dharma demonstrates through a living enlightened civilization that global peace is achievable and sustainable, and this begins with individual peace and spiritual awakening; and

WHEREAS, during the month of October, the culture, history, traditions, achievements and contributions of Hindu Americans are recognized, and celebrated throughout the United States of America, the State of California, and the City of Redlands; and

WHEREAS, the City of Redlands values diversity, the variety of cultural traditions and encourages its citizens to better understand, recognize and celebrate the rich history and shared experiences of Hindu Americans; and

WHEREAS, across our City of Redlands, Hindu Americans have filled our communities with rich traditions, and abundant culture and the City is proud to recognize, during Hindu Heritage Month, their many social, cultural and economic contributions to our city, state and nation;

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Redlands does hereby recognize the month of October 2026, as Hindu Heritage month in the City of Redlands. The City of Redlands encourages residents, educational institutions, and community organizations to observe Hindu Heritage Month through activities, events, and educational initiatives that promote understanding, cultural exchange, and respect for Hindu traditions and contributions.

IN WITNESS WHEREOF, we hereunto affix our signatures and Official Seal of the City of Redlands on this 6th day of October 2026.

_____

Mario Saucedo, Mayor

Attest:

_____

Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. I4.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve an Intergovernmental Purchase of Palo Alto Networks Firewall Software Support for One Year from Sidepath, Inc. in the amount of $100,100 (Assistant City Manager Garcia)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move to approve an intergovernmental purchase of Palo Alto Networks Firewall Software Support for one year from Sidepath, Inc. in the amount of $100,100.

RECOMMENDATION:

Staff recommends that the City Council approve an intergovernmental purchase of Palo Alto Networks Firewall Software Support for one year from Sidepath, Inc. in the amount of $100,100.

DISCUSSION:

In 2023, the City's Division of Innovation and Technology (DoIT) procured four Palo Alto Networks firewalls. Palo Alto firewalls are known and widely utilized for their advanced threat detection and prevention capabilities, and provide high visibility into application-level traffic and allow for complex security configurations. These firewalls are designed to handle high-volume network traffic and offer scalability options to accommodate future growth, which the City has experienced since their purchase.

The initial purchase of the firewalls in 2023 included three years of support, but this will now need to be procured and renewed annually while this hardware is in service. Using an intergovernmental agreement, DoIT is proposing the purchase of one year of support for these firewalls from Sidepath, Inc. This software and technical support is available at all times and includes advanced security subscriptions that provide tools to customize the City's security infrastructure. The subscriptions will also provide the City with upgrades and maintenance updates for the firewalls that will allow the City to adapt to ever-evolving threats that municipalities now frequently encounter.

Staff followed the City's procurement guidelines by examining and selecting an existing competitively bid cooperative contract with the National Association of State Procurement Officials (NASPO) ValuePoint. NASPO is a non-profit association made up of the directors of the central purchasing offices of the 50 states, the District of Columbia and territories of the United States. By utilizing the NASPO ValuePoint cooperative purchasing, the City is able to benefit from the combined purchasing power of more than 50,000 government, educational, and non-profit organizations. The purpose of these cooperative contract programs is to enable the City to take advantage of preferred pricing and administrative efficiencies. Based on staff's assessment, the proposed purchase for software support is recommended to be sourced through this cooperative purchasing agreement.

ALTERNATIVES:

City Council may choose to reject, modify, or table the proposed purchase. However, the purchase is recommended in order to maintain the City's network security posture and mitigate the risks associated with modern cyber threats.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Danielle Garcia, Assistant City Manager

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Kurt Wilson, Assistant City Manager
James Garland, Finance Director
Dana Abramovitz-Daniel, Procurement Manager

PREPARED BY:
Valerie Abrego, Management Analyst

FISCAL IMPACT

Fiscal Year: 2027

Revenue Generating: No

Amount: $100,100.00

Budgeted Y/N: Y

Account No.: 604900

Additional Appropriation Required: No

Discussion: Funding for this was included in the FY27 budget for Management Services/DoIT.

Attachments

NASPO_CA_Addendum.pdf
Intergovernmental_Request_Form-Sidepath-Palo_Alto-_MS.pdf
NASPO_Master_Agreement.pdf
Sidepath_PA_Support_Quote.pdf
NASPO_Portfolio_Snapshot.pdf

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-17-70-40-05
AMENDMENT 4

Cloud Solutions
Utah NASPO ValuePoint Master Agreement Number AR2472
Carahsoft Technology Corp. (Contractor)

The parties mutually agree to amend Participating Addendum 7-17-70-40-05 as follows:

1) **Section 19. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING** is hereby added to read as follows:

19. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING

The State of California seeks to realize the potential benefits of GenAI, through the development and deployment of GenAI tools, while balancing the risks of these new technologies.

Upon request by an ordering agency, Contractor must complete a GenAI Reporting and Fact Sheet (STD 1000) to identify if their solution or service includes, or makes available, any GenAI including, GenAI from third parties or subcontractors.

During the term of the contract, Contractor must notify the State in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000) to notify the State of any new or previously unreported GenAI technology.

At the direction of the State, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk or contract performance, until use of such GenAI technology has been approved by the State.

Failure to disclose GenAI use to the State and submit the GenAI Reporting and Factsheet (STD 1000) may be considered a breach of the contract by the State at its sole discretion and the State may consider such failure to disclose GenAI and/or failure to submit the GenAI Reporting and Factsheet (STD 1000) as grounds for the immediate termination of the contract. The State is entitled to seek any and all relief to which it may be entitled to as a result of such non-disclosure.

The State reserves the right to amend the contract, without additional cost, to incorporate GenAI Special Provisions into the contract at its sole discretion and/or terminate any contract that presents an unacceptable level of risk to the State.

If Contractor identifies GenAI in their solution, a copy of the STD 1000 must be submitted to the DGS State Contract Administrator.

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the date of execution by both parties below.

STATE OF CALIFORNIA	**CONTRACTOR**
Department of General Services	Carahsoft Technology Corp.
Agency Name	*Contractor Name*
Julie Matthews Digitally signed by Julie Matthews Date: 2024.12.20 13:39:21 -08'00' 12/20/2024	Madeline Hall 12/13/2024
Authorized Signature *Date Signed*	*Authorized Signature* *Date Signed*
Julie Matthews, MAU2 Supervisor	Madeline Hall, Contracts Manager
Printed Name/Title of Person Signing	*Printed Name/Title of Person Signing*
707 Third Street West Sacramento, CA 95605	11493 Sunset Hills Road, Suite 100 Reston, VA 20190
Address	*Address*

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-17-70-40-05
AMENDMENT 3

Cloud Solutions

Utah NASPO ValuePoint Master Agreement Number AR2472

Carahsoft Technology Corporation (Contractor)

The parties mutually agree to amend Participating Addendum 7-17-70-40-05 as follows:

1) **Section 7. PRICING** is revised to read as follows:

   A. Contractor's pricing is outlined in the Utah NASPO ValuePoint Master Agreement Number AR2472.

2) **Section 16. CONTRACT MANAGEMENT, subparagraph A** is revised to read as follows:

   A. The primary Contractor Contract Manager for this Participating Addendum shall be as follows:

Contractor	**Contract Manager**
Name:	Mariah Edwards
Phone:	(818) 449-3729
Email:	Mariah.Edwards@carahsoft.com
Address:	Carahsoft Technology Corporation Mariah Edwards 11493 Sunset Hills Road, Suite 100 Resto, VA 20190

3) **Section 18. EXECUTIVE ORDER N-6-22 – RUSSIA SANCTIONS** is hereby added to read as follows:

18. EXECUTIVE ORDER N-6-22 – RUSSIA SANCTIONS

On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. "Economic Sanctions" refers to sanctions imposed by the U.S. government in response to Russia's actions in Ukraine, as well as any sanctions imposed under state law. The EO directs state agencies to terminate contracts with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that shall be grounds for termination of this Participating Addendum. The State shall provide Contractor advance written notice of such termination, allowing Contractor at least thirty (30) calendar days to provide a written response. Termination shall be at the sole discretion of the State.

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the date of execution by both parties below.

STATE OF CALIFORNIA	**CONTRACTOR**
Department of General Services	Carahsoft Technology Corporation
Agency Name	*Contractor Name*
Julie Matthews Digitally signed by Julie Matthews Date: 2023.06.29 16:09:08 -07'00' 6/29/2023	Kristina Smith 06/22/2023
Authorized Signature *Date Signed*	*Authorized Signature* *Date Signed*
Julie Matthews, MAU2 Supervisor	Kristina Smith, Contracts Director
Printed Name/Title of Person Signing	*Printed Name/Title of Person Signing*
707 Third Street West Sacramento, CA 95605	11493 Sunset Hills Rd, Suite 100, Reston, VA 20190
Address	*Address*

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-17-70-40-05
AMENDMENT 2

Cloud Solutions
Utah NASPO ValuePoint Master Agreement Number AR2472
Carahsoft Technology Corp. (Contractor)

The parties mutually agree to amend Participating Addendum 7-17-70-40-05 as follows:

1) **Section 3. TERMS AND CONDITIONS/INCORPORATION OF DOCUMENTS** is updated to read as follows:

   A. Terms and conditions listed below are hereby incorporated by reference and made a part of this Participating Addendum as if attached herein and shall apply to the purchase of goods or services made under this Participating Addendum. Terms can be viewed on the DGS Procurement Division website (https://www.dgs.ca.gov/PD/Resources/Page-Content/Procurement-Division-Resources-List-Folder/Model-Contract-Language).

      i. General Provisions – Information Technology (GSPD-401IT) effective 9/5/2014.
      ii. Cloud Computing Software as a Service (SaaS) General Provisions effective 6/7/2019.
      iii. Cloud Computing Special Provisions for Software as a Service (SaaS) effective 03/15/18.
      iv. Cloud Computing Special Provisions for Infrastructure as a Service (IaaS) & Platform as a Service (PaaS), effective 05/11/16.

2) **Section 5. AVAILABLE PRODUCTS AND SERVICES** is updated to read as follows:

   A. The following service offerings from the Utah NASPO ValuePoint Master Agreement Number AR2472 are allowed under this Participating Addendum:

      1) Software as a Service (SaaS)
      2) Infrastructure as a Service (IaaS)
      3) Platform as a Service (PaaS)

3) **Section 6. RESTRICTIONS/DISALLOWED PRODUCTS AND SERVICES (STATE AGENCIES ONLY)** is updated to read as follows:

   A. The following product/service offerings are disallowed for state agencies under this Participating Addendum:

      1) Value Added Services, including Additional Value Added Services such as Maintenance Services; Deployment Services; Consulting/Advisory Services; Architectural Design Services; Statement of Work Services; Partner Services, and Training Deployment Services

B. Product and service categories that are available on mandatory California statewide contracts cannot be purchased from this Participating Addendum by State agencies without an exemption. Prior to issuing a purchase order, State agencies are responsible for obtaining an exemption from DGS, and/or California Department of Technology (CDT).

C. State agencies must first obtain approval by the California Department of Technology (CDT) to use this Participating Addendum for Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) purchases in accordance with Technology Letter 17-06 (www.cdt.ca.gov/wp-content/uploads/2017/08/TL-17-06.pdf).

4) **Section 14. CONTRACT MANAGEMENT subpart A** is updated to read as follows:

A. The primary Contractor Contract Manager for this Participating Addendum shall be as follows:

Contractor:	Carahsoft Technology Corp.
Name:	Alex Cord
Phone:	703-871-8500
E-Mail:	Alex.Cord@Carahsoft.com
Address:	11493 Sunset Hills Road, Suite 100 Reston, VA 20190

5) **Section 9 FULFILLMENT PARTNERS/AUTHORIZED RESELLERS** is updated to read as follows:

A. Contractor may use State-approved Authorized Resellers under this Participating Addendum for sales and service functions as defined herein.

1) Orders may be placed with the Contractor or Authorized Resellers.

2) Authorized Resellers must accept purchase orders and accept payment from ordering agencies for products and services offered under this Participating Addendum.

3) Authorized Resellers are responsible for sending a copy of all purchase orders and invoices to the Contractor for compliance with quarterly usage reporting and administrative fee requirements.

4) All purchase documents to Authorized Resellers shall reference the Participating Addendum Number and Contractor Name.

B. Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions under this Participating Addendum, even if work is performed by Authorized Resellers. All State policies, guidelines, and requirements shall apply to Authorized Resellers.

C. Contractor will be the sole point of contact with regard to Participating Addendum contractual matters, reporting, and administrative fee requirements.

D. Subject to the approval of the State, Authorized Resellers may be added on a quarterly basis during the term of the contract. Contractors shall notify the State of any deleted Authorized Resellers or changes to current Authorized Resellers' contact information in writing at any time during the contract term.

E. Contractor will be required to submit Authorized Reseller requests, in a format specified by the State, to the State Contract Administrator for approval.

F. State-approved Authorized Resellers will be posted on the State's Cal eProcure website.

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the date of execution by both parties below.

STATE OF CALIFORNIA		**CONTRACTOR**	
Department of General Services		Carahsoft Technology Corp.	
Agency Name		*Contractor Name*	
	August 11, 2021	Kristina Smith	8/11/2021
Authorized Signature	*Date Signed*	*Authorized Signature*	*Date Signed*
Stephanne Lim, MAU2 Supervisor		Kristina Smith - Director of Contracts	
Printed Name/Title of Person Signing		*Printed Name/Title of Person Signing*	
707 Third Street West Sacramento, CA 95605		11493 Sunset Hills Road, Suite 100 Reston, VA 20190	
Address		*Address*	

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NO. 7-17-70-40-05
AMENDMENT NO. 1

Cloud Solutions
Utah NASPO ValuePoint Master Agreement No. AR2472
Carahsoft Technology Corp.

The parties hereto mutually agree to amend Participating Addendum Number 7-17-70-40-05 as follows:

1. Authorized Resellers outlined in Section 9 (Fulfillment Partners/Authorized Resellers) is revised to reflect the following:

Authorized Resellers are available for this Participating Addendum:

ISSUE PURCHASE ORDER TO

Orders may be placed with Carahsoft Technology Corp. or with an Authorized Reseller as indicated below:

Orders placed with Carahsoft Technology Corp.

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
1860 Michael Faraday Drive, Suite 100 Tempe, AZ 85283

Contact: Karina Woods
Phone: 703/871-8500
Fax No.: 703/871-8505
E-mail: OM@carahsoft.com

Orders placed with an Authorized Reseller must be addressed as shown below, and payment must be made payable to the Authorized Reseller identified on the invoice as shown below:

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Allied Network Solutions, Inc.
5718 Lonetree Blvd., Rocklin, CA 95765

Contact: Roger Schnorenberg
Phone: 916/774-2670 X101
E-mail: Rschnorenberg@ans-it.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Data Path Inc.
318 McHenry Ave., Modesto, CA 95354

Contact: Brian Jump
Phone: 209/312-9808
E-mail: BJump@mydatapath.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o DynTek Services, Inc.
4440 Von Karman, Suite 200, Newport Beach, CA 92660

Contact: Kelsea Pratt-Acosta
Phone: 949/271-6780
Fax No.: 949/271-6794
E-mail: CAsales@dyntek.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Eventus Solutions Group LLC
9777 Pyramiel Court, Suite 160, Englewood, CA 80112

Contact: Craig Tobin
Phone: 303/376-6161
E-mail: Craigtobin@eventusg.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o HF Tech Services, Inc.
5777 Madison Avenue, Suite 1060, Sacramento, CA 95841

Contact: Allan P. Hart
Phone: 916/690-5056
E-mail: allan@hftechservices.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o NWN Solutions Corporation
2969 Prospect Park Drive, Suite 225, Rancho Cordova, CA 95670

Contact: Team Meade
Phone: 916/637-2160
Fax No.: 916/596-4800
E-mail: TMeade@nwnit.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Savant Solutions, Inc. which will do business in California as [Savant Solutions Group]
1931 H Street, Sacramento, CA 95811

Contact: Caleb Kwong
Phone: 916/836-8182
E-mail: Caleb@savantsolutions.net

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o SHI International, Corp.
290 Davidson Avenue, Somerset, NJ 08873

Contact: Nick Grappone
Phone: 732/564-8189
E-mail: Nick_Grappone@shi.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Solutions Simplfied
8880 Cal Center Drive, Suite 400, Sacramento, CA 95826

Contact: Rachel DaValle
Phone: 530/521-0576
E-mail: Rachel.Davalle@solutionssimplified.net

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Taborda Solutions, Inc.
9580 Oak Ave Pkwy, Suite 7-180, Folsom, CA 95630

Contact: Bear Williams
Phone: 916/717-8711
Fax No.: 916/200-0353
E-mail: Bear.Williams@tabordasolutions.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o vCloud Tech Inc.
609 Deep Valley Drive, Suite 200, Rollling Hills Estates, CA 90274

Contact: Nadia Khan
Phone: 424/703-4135
E-mail: nadiakhan@vcloudtech.com

For invoicing purposes, each State Accounting office must have a copy of the reseller's Payee Data Record (Std. 204) in order to process payment of the invoice. Agencies should forward a copy of the Std. 204 to their respective accounting office. Without the Std. 204, payment may be unnecessarily delayed.

AUTHORIZED RESELLERS ARE RESPONSIBLE FOR SENDING A COPY OF ALL PURCHASE ORDERS TO QUEST MEDIA & SUPPLIES, INC. FOR COOPERATIVE AGREEMENTS (NASPO VALUEPOINT) QUARTERLY REPORTING REQUIREMENTS. When issuing an order to an authorized reseller listed on Cooperative Agreements, it is the agency's responsibility to ensure that the reseller holds a valid California Seller's Permit.

NOTE: Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions under this Participating Addendum, even if work is performed by Authorized Resellers. All State policies, guidelines, and requirements shall apply to Authorized Resellers.

All other terms and conditions of the Participating Addendum shall remain the same.

IN WITNESS WHEREOF, the parties have executed this Participating Addendum Amendment as of the date of execution by both parties below.

Participating State:
State of California,
Department of General Services

By: _____

for Name: Angela Shell

Title: Deputy Director

Date: May 1, 2018

Contractor:
Carahsoft Technology Corp.

By: _____

Name: Robert R. Moore

Title: Vice President

Date: April 25, 2018

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NO. 7-17-70-40-05

Cloud Solutions

Utah NASPO ValuePoint Master Agreement No. AR2472

Carahsoft Technology Corp.

This Participating Addendum Number 7-17-70-40-05 is entered into between the State of California, Department of General Services (hereafter referred to as "State" or "DGS") and Carahsoft Technology Corp. (hereafter referred to as "Contractor") under the lead State of Utah NASPO ValuePoint Master Agreement Number AR2472.

1. SCOPE

A. This Participating Addendum covers the purchase of Cloud Solutions under the Utah NASPO ValuePoint Master Agreement. The Utah NASPO ValuePoint Master Agreement Number AR2472 is hereby incorporated by reference. The cloud solution services are identified in Section 5 (Available Services).

B. This Participating Addendum is available for use by all State Agencies including the Executive, Judicial and Legislative branches, and will include all California political subdivisions/local governments. A subdivision/local government is defined as any city, county, city and county, district, or other local governmental body or corporation, including the California State Universities (CSU) and University of California (UC) systems, K-12 schools and community colleges empowered to expend public funds.

C. Each political subdivision/local government is to make its own determination whether this Participating Addendum and the Utah NASPO ValuePoint Master Agreement are consistent with its procurement policies and regulations.

2. TERM

A. The term of this Participating Addendum shall begin upon signature approval by the State and will end September 15, 2026, or upon termination by the State, whichever occurs first.

B. Lead State amendments to extend the Master Price Agreement term date are not automatically incorporated into this Participating Addendum. Extension(s) to the term of this Participating Addendum will be through a written amendment upon mutual agreement between the State and the Contractor.

3. TERMS AND CONDITIONS/INCORPORATION OF DOCUMENTS

A. Terms and conditions listed below are hereby incorporated by reference and made a part of this Participating Addendum as if attached herein and shall apply to the purchase of services made under this Participating Addendum.

1) **General Provisions – Information Technology (GSPD-401IT),** effective 9/5/2014. The twelve (12) page document can be viewed at: http://www.documents.dgs.ca.gov/pd/poliproc/GSPD401IT14_0905.pdf. Exception: Article 11 of the General Provisions – Information Technology, is superseded by Section 4 (Order of Precedence) below.

2) **Cloud Computing Special Provisions for Software as a Service (SaaS),** effective 9/3/14. The five (5) page document can be viewed at: http://www.documents.dgs.ca.gov/pd/poliproc/CLOUDCOMPUTINGSERVICESSPECIALPROVISIONS_14_0903.docx

4. ORDER OF PRECEDENCE

In the event of any inconsistency between the articles, attachments, or provisions which constitute this agreement, the following descending order of precedence shall apply:

A. California Participating Addendum Number 7-17-70-40-05
B. Utah NASPO ValuePoint Master Agreement Number AR2472
C. Utah Solicitation CH16012 including all Addendums
D. Contractor's response to Utah's Solicitation

5. AVAILABLE SERVICES

The following service offering from the Utah NASPO ValuePoint Master Agreement Number AR2472 are allowed under this Participating Addendum:

Software as a Service (SaaS)

6. RESTRICTIONS/DISALLOWED SERVICES – These restrictions are not applicable to political subdivisions/local governments.

A. The following service offerings are prohibited under this Participating Addendum:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Value Added Services, including Additional Value Added Services such as Maintenance Services; Deployment Services; Consulting/Advisory Services; Architectural Design Services; Statement of Work Services; Partner Services, and Training Deployment Services

B. Product and service categories that are available on mandatory California statewide contracts cannot be purchased from this Participating Addendum by State Departments without an exemption. Prior to issuing a purchase order, State Departments are responsible for obtaining an exemption from DGS, and/or California Department of Technology (CDT).

7. PRICING

A. Contractor shall submit a Price Schedule identifying all services offered under this Participating Addendum for the State's approval.

B. The Price Schedule shall include the following:

1) Service Category (SaaS) Description
2) List Price
3) Discount off List Price
4) Contract Price

C. Contractor shall obtain prior approval from Utah NASPO ValuePoint Contract Administrator, and submit a written notice of price increases/decreases and a revised Price List for the State's approval.

D. State-approved Price List will be posted on the State's Cal eProcure website.

8. SERVICE ADDITIONS/DELETIONS

A. Contractor may add or delete services introduced or removed from the market by the manufacturer under the following conditions:

1) Service is within existing awarded categories under the NASPO ValuePoint Master Price Agreement;
2) Contractor has obtained prior approval from the Utah NASPO ValuePoint Contract Administrator; and
3) Contractor receives written approval from the California State Contract Administrator.

B. Contractor shall submit a written notice of service (s) additions/deletions and a revised Price Schedule for the State's approval.

9. FULFILLMENT PARTNERS/AUTHORIZED RESELLERS

Authorized Resellers are available for this Participating Addendum:

ISSUE PURCHASE ORDER TO

Orders may be placed with Carahsoft Technology Corp. or with an Authorized Reseller as indicated below:

Orders placed with Carahsoft Technology Corp.

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
1860 Michael Faraday Drive, Suite 100

Contact: Karina Woods
Phone: 703/871-8500
Fax No.: 703/871-8505
E-mail: OM@carahsoft.com

Orders placed with an Authorized Reseller must be addressed as shown below, and payment must be made payable to the Authorized Reseller identified on the invoice as shown below:

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o DynTek Services, Inc.
4440 Von Karman, Suite 200, Newport Beach, CA 92660

Contact: Kelsea Pratt-Acosta
Phone: 949/271-6780
Fax No.: 949/271-6794
E-mail: CAsales@dyntek.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o NWN Solutions Corporation
2969 Prospect Park Drive, Suite 225, Rancho Cordova, CA 95670

Contact: Team Meade
Phone: 916/637-2160
Fax No.: 916/596-4800
E-mail: TMeade@nwnit.com

SUBMIT ORDERS TO:

Carahsoft Technology Corp.
c/o Taborda Solutions, Inc.
9580 Oak Ave Pkwy, Suite 7-180, Folsom, CA 95630

Contact: Bear Williams
Phone: 916/717-8711
Fax No.: 916/200-0353
E-mail: bear.williams@tabordasolutions.com

For invoicing purposes, each State Accounting office must have a copy of the reseller's Payee Data Record (Std. 204) in order to process payment of the invoice. Agencies should forward a copy of the Std. 204 to their respective accounting office. Without the Std. 204, payment may be unnecessarily delayed.

AUTHORIZED RESELLERS ARE RESPONSIBLE FOR SENDING A COPY OF ALL PURCHASE ORDERS TO CARAHSOFT TECHNOLOGY CORP. FOR COOPERATIVE AGREEMENTS (NASPO VALUEPOINT) QUARTERLY REPORTING REQUIREMENTS.

When issuing an order to an authorized reseller listed on Cooperative Agreements, it is the agency's responsibility to ensure that the reseller holds a valid California Seller's Permit.

NOTE: Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions under this Participating Addendum, even if work is performed by Servicing Subcontractors. All State policies, guidelines, and requirements shall apply to Authorized Resellers.

10. ORDERING AGENCY RESPONSIBILITIES

A. State department and political subdivision/local government use of this Participating Addendum is optional.

B. State departments and political subdivision/local governments must follow the ordering procedures outlined within the User Instructions guide, administered by the State Contract Administrator, to execute orders against this Participating Addendum.

11. INVOICING AND PAYMENT

A. Payment terms for this Participating Addendum are net forty-five (45) days. Payment will be made in accordance with IT General Provisions Paragraph 30 (Required Payment Date).

B. Invoices shall be sent to the address identified in the Ordering Agency's purchase order. The State Participating Addendum Number and Ordering Agency Purchase Order Number shall appear on each invoice for all purchases placed under this Participating Addendum.

C. Contractor will accept the State of California credit card (CAL-Card) for payment of invoices.

12. USAGE REPORTING

A. Contractor shall submit usage reports on a quarterly basis to the State Contract Administrator for all California entity purchases using the report template attached hereto as Attachment A. The report is due even when there is no activity.

B. The report shall be an Excel spreadsheet transmitted electronically to the DGS mailbox at PDCooperatives@dgs.ca.gov.

C. Any report that does not follow the required format or that excludes information will be deemed incomplete. Contractor will be responsible for submitting corrected reports within five business days of the date of written notification from the State.

D. Tax must not be included in the report, even if it is on the purchase order.

E. Reports are due for each quarter as follows:

Reporting Period	Due Date
JUL 1 to SEP 30	OCT 31
OCT 1 to DEC 31	JAN 31
JAN 1 to MAR 31	APR 30
APR 1 to JUN 30	JUL 31

F. Failure to meet reporting requirements and submit the reports on a timely basis shall constitute grounds for suspension of this contract.

G. Amendments for term extensions may be approved only if all due reports have been submitted to the State.

13. ADMINISTRATIVE FEE

A. Contractor shall submit a check, payable to the State of California, remitted to the Cooperative Agreement Unit for the calculated amount equal to one percent (0.01) of the sales for the quarterly period.

B. Contractor must include the Participating Addendum Number on the check. Those checks submitted to the State without the Participating Addendum Number will be returned to Contractor for additional identifying information.

C. Administrative fee checks shall be submitted to:

State of California
Department of General Services, Procurement Division
Attention: Cooperative Agreement Program
707 3rd Street, 2nd Floor, MS 2-202
West Sacramento, CA 95605

D. The administrative fee shall not be included as an adjustment to Contractor's NASPO ValuePoint Master Agreement pricing.

E. The administrative fee shall not be invoiced or charged to the ordering agency.

F. Payment of the administrative fee is due irrespective of payment status on orders or service contracts from a purchasing entity.

G. Administrative fee checks are due for each quarter as follows:

JUL 1 to SEP 30	OCT 31
OCT 1 to DEC 31	JAN 31
JAN 1 to MAR 31	APR 30
APR 1 to JUN 30	JUL 31

H. Failure to meet administrative fee requirements and submit fees on a timely basis shall constitute grounds for suspension of this contract.

14. CONTRACT MANAGEMENT

A. The primary Contractor Contract Manager for this Participating Addendum shall be as follows:

Contractor:	Carahsoft Technology Corp.
Name:	Jack Dixon
Phone:	703-230-7545
Fax:	703-871-8505
E-Mail:	naspo@carahsoft.com
Address:	1860 Michael Faraday Drive, Ste 100 Reston, VA 20190

B. The State Contract Administrator for this Participating Addendum shall be as follows:

Name:	Yolanda Tutt
Phone:	916.375.4408
Fax:	916.375.4663
E-Mail:	yolanda.tutt@dgs.ca.gov
Address:	State of California Department of General Services Procurement Division 707 Third Street, 2nd Floor, MS 2-202 West Sacramento, CA 95605

C. Should the contact information for either party change, the party will provide written notice with updated information no later than ten business days after the change.

15. Termination of Agreement

The State may terminate this Participating Addendum at any time upon 30 days prior written notice to the Contractor. Upon termination or other expiration of this Participating Addendum, each party will assist the other party in orderly termination of the Participating Addendum and the transfer of all assets, tangible and intangible, as may facilitate the orderly, nondisrupted business continuation of each party. This provision shall not relieve the Contractor of the obligation to perform under any purchase order or other similar ordering document executed prior to the termination becoming effective.

16. Amendment

No amendment or variation of the terms of this Participating Addendum shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or agreement not incorporated in the Participating Addendum is binding on any of the parties.

17. Agreement

A. This Participating Addendum and the Master Agreement together with its exhibits and/or amendments, set forth the entire agreement between the parties with respect to the subject matter of all previous communications, representations or agreements, whether oral or written, with respect to the subject matter hereof. Terms and conditions inconsistent with, contrary or in addition to the terms and conditions of this Participating Addendum and the Master Agreement, together with its exhibits and/or amendments, shall not be added to or incorporated into this Participating Addendum or the Master Agreement and its exhibits and/or amendments, by any subsequent purchase order or otherwise, and any such attempts to add or incorporate such terms and conditions are hereby rejected. The terms and conditions of this Participating Addendum and the Master Agreement and its exhibits and/or amendments shall prevail and govern in the case of any such inconsistent or additional terms.

B. By signing below Contractor agrees to offer the same services as on the Utah NASPO ValuePoint Master Agreement Number AR2472, at prices equal to or lower than the prices on that contract.

C. IN WITNESS WHEREOF, the parties have executed this Participating Addendum as of the date of execution by both parties below.

STATE OF CALIFORNIA	CONTRACTOR
Department of General Services	Carahsoft Technology Corp.
Agency Name	*Contractor Name*
Rhonda Smith 9/15/2017	August 9, 2017
Signature of Authorized Signer *Date Signed*	*Signature of Authorized Signer* *Date Signed*
Ricardo Martinez, Acting Deputy Director	Ellen Lord, Contracts Manager
Printed Name and Title of Authorized Signer	*Printed Name and Title of Authorized Signer*
707 Third Street West Sacramento, CA 95605	1860 Michael Faraday Drive, Suite 100 Reston, VA 20190
Address	*Address*

Participating Addendum No.
Attachment A
Sheet 1 of 1

Contract Number:	
Contractor:	
Reporting Period:	
Report Value:	
Administrative Fee:	

Ordering Agency Full Name	State/Local Spend	Purchase Order / Service Contract Number	Order Date	Category ID	Manufacturer Part Number (OEM #)	Item Description	Unit of Measure	Quantity in Unit of Measure	Quantity	List Price/MSRP	Contract Unit Price	Extended Contract Price Paid	Index Date / Catalog Version

Intergovernmental/ Piggyback Contract Use Request

(Attach to PR form)

The Management Services- DoIT Department requests the purchase of the following item(s) from:

Original Contracting Entity: Utah National Association of State Procurement Officials (NASPO)
Contract#: C0000116540 Utah NASP ValuePoint Master Agreement #AR2472 California Participating Addendum Number 7-17-70-40-05
Contract Term: October 15, 2016- January 13, 2027
Method of original contract award: ☑ Competitive ☐ Non-Competitive, based on: ☐ Preferred source ☐ Sole ☐ Single source ☐ Emergency ☐ Other:
Does the original contract contain language contemplating contract extension to additional users? ☑ Yes ☐ No

Please attach: vendor agreement to sale to the City AND Entity agreement/contract language allowing Piggyback

Description of Product/Service intend to acquire	Unit Price	Total
Qty: 2- Palo Alto Prisma Access Agent Subscription- 1 Year	$ 3,169.89	$ 6,339.78
Qty: 4- Precision AI Network Security Subscription Renewal- 1 Year	$ 18,175.43	$ 72,701.72
Qty: 4-Premium Support- 1 Year	$ 3,898.35	$ 15,593.40
Qty: 2-Palo Alto Prisma Access Agent Subscription- 1 Year	$ 3,182.25	$ 6,364.50
Tax	$ 0.00	
	Grand Total	$ 100,999.40

Vendor:	Sidepath
Contact:	Catherine Paull
Address 1:	22892 Mill Creek Drive
Address 2:	
City/State/Zip:	Laguna Hills, CA 92653
Telephone:	949-748-8700
Fax:	949-748-8706
Web/E-Mail:	www.sidepath,com

Delivery/Service Location	
Contact:	Eric Owens
Telephone:	909-335-4798
Department:	Management Services
Address 1:	35 Cajon St., Suite 222
Address 2:	Redlands, CA 92373
Additional Comments	

Purchasing Agent Approval: _____ Date: _____

City Manager Approval: _____ Date: _____

Contract # AR2472

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Division of Purchasing and the following Contractor:

Carahsoft Technology Corporation
Name
1860 Michael Faraday Drive, Suite 100
Address

Reston	VA	20190
City	State	Zip

LEGAL STATUS OF CONTRACTOR
- ☐ Sole Proprietor
- ☐ Non-Profit Corporation
- ☒ For-Profit Corporation
- ☐ Partnership
- ☐ Government Agency

Contact Person Bethany Blackwell Phone #703-230-7435 Email NASPO@carahsoft.com
Vendor #VC0000116540 Commodity Code #920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed

3. PROCUREMENT PROCESS: This contract is entered into as a result of the procurement process on Bid#CH16012.

4. CONTRACT PERIOD: Effective Date: 10/14/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.

5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
ATTACHMENT E: Service Offering EULAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah State Procurement Code and the Procurement Rules.

9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Contractor's signature	10/11/16 Date

Robert Moore, Vice President
Type or Print Name and Title

STATE

for Director, Division of Purchasing	10.13.16 Date

Christopher Hughes	801-538-3254		christopherhughes@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

(Revision 16 June 2016)

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.

Master Agreement.

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run

arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures

specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement

and an amendment is not necessary.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing

Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

13. Indemnification and Limitation of Liability

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, bodily injury, or damage to real or tangible property arising directly or indirectly from the negligent or wrongful act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any

person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to:

a. Any use of the Services provided hereunder not contemplated in the product documentation.
b. Any use of the Services provided hereunder in combination with other products not contemplated hereunder or in the documentation, any use of modification of the Services provided hereunder except as permitted by this Agreement.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

b. Except as otherwise set forth in the Indemnification Paragraphs above, the limit of liability shall be as follows:

i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable

Purchase Order) or (ii) two million dollars ($2,000,000), whichever is greater.
ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.
iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in Section 43 will not apply to claims for bodily injury or death as set forth in Section 13, and Section 30 when made applicable under a specific purchase order.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage	**Crime Insurance** Minimum Insurance Coverage
Low	$2,000,000	$2,000,000

Moderate	$5,000,000	$5,000,000
High	$10,000,000	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage

may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

The federal and state laws, regulations, policies, standards, and guidelines that Contractors doing business with the Participating Entities must be aware of, include, but not limited to: Criminal Justice Information Services (CJIS) Security Policy; Federal Educational Rights and Privacy Act (FERPA); Federal Information Security Management Act (FISMA); National Institute of Technology Standards; Gramm-Leach-Bliley Act (GLB) Act; Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Health Act (HITECH); IRS Publication 1075; Payment Card Industry Data Security Standard (PCI DSS); Sarbanes-Oxley Act (SOX); Electronic Communications Privacy Act, Stored Communications Act and the PATRIOT Act. The list is intentionally United States-centric, and is not intended to be all-inclusive. Further, since laws, regulations, requirements and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical. Many State Entities have additional program compliance requirements that must be considered in addressing compliance. (e.g., DMV Privacy Act, Public Service Law, etc.).

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized

by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

subsection must be consistent with license rights granted for use of intellectual property.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation. Contractor must maintain any certifications required under the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the

Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: When required by a specific purchase order issued under this Agreement or a Participating Addendum and accepted by the Contractor, the Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and

Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have

additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://www.naspo.org/WNCPO/Calculator.aspx. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) Ship Date; (8) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment F.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list

of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:**

   a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

   b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

   c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. **Personal Data Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

   a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

   b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3)

document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests**: If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law. .

7. **Termination and Suspension of Service**:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- • 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD,

backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:** Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:** The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Right to Remove Individuals:** The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately

remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:** The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

    a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

    b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

    c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 48 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

    a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests**: If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law.

7. **Termination and Suspension of Service**:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of

Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:**

    a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

    b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

    c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:**

    a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

    b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon

request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.
16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:** The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

   a. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

   b. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

   a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

   b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident

review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests**: If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law.

7. **Termination and Suspension of Service**:

   a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

   b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

   c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

   d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

   e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:**

   a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty,

including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:**

   a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing

   b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.
11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that

may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.
17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement via amendment.

Attachment B – Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Service Model:	**Low Risk Data**	**Moderate Risk Data**	**High Risk Data**	**Deployment Models Offered:**
Saas	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
IaaS	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	FireEye, Google, QTS, Virtustream, VMware
PaaS	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Google, QTS, Salesforce, SAP, ServiceNow, Virtustream

Carahsoft's solution providers each have different forms and procedures for providing solutions and services with varying levels of data management for each solution. Please see Carahsoft's Technical Response for additional information regarding risk data management of low, moderate, and high risk data.

Attachment C – Cost Schedule

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

Cloud Solutions By Category. Specify ***Discount Percent %*** Offered for products in each category. Highest discount will apply for products referenced in detail listings for multiple categories. Provide a detailed product offering for each category.

Software as a Service **Discount % 0-21.60**

Infrastructure as a Service **Discount % _0-10__**

Platform as a Services **Discount % _0-11__**

Value Added Services **Discount % _0-13__**

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate $ _250_____
Remote Hourly Rate $ _175_____

Professional Services

- **Deployment Services** — **Onsite Hourly Rate $ __350_____** / **Remote Hourly Rate $ _275_____**
- **Consulting/Advisory Services** — **Onsite Hourly Rate $ __300_____** / **Remote Hourly Rate $ _225_____**
- **Architectural Design Services** — **Onsite Hourly Rate $ __300_____** / **Remote Hourly Rate $ _225_____**
- **Statement of Work Services** — **Onsite Hourly Rate $ __250_____** / **Remote Hourly Rate $ _175_____**

Partner Services **Onsite Hourly Rate $ ___250_____**
Remote Hourly Rate $ __175_____

Training Deployment Services **Onsite Hourly Rate $ ___250_____**
Online Hourly Rate $ ___175_____

Manufacturer	Description	Vendor Part No	List Price	GSA Price
AODocs	AODOCS-TEAM-FOLDERS-12MO	AODocs Team Folders: 12 mo	$ 36.00	$ 35.19
AODocs	AODOCS-DOCUMENT-MANAGEMENT-12MO	AODocs Document Managen	$ 72.00	$ 70.38
AODocs	AODOCS-TEAM-FOLDERS-1MO	AODocs Team Folders: 1 mo	$ 3.00	$ 2.93
AODocs	AODOCS-DOCUMENT-MANAGEMENT-1MO	AODocs Document Managen	$ 6.00	$ 5.87
AODocs	AODOCS-RETENTION-12MO	AODocs Retention Managem	$ 30.00	$ 29.33
AODocs	AODOCS-EMAIL-CONNECTOR-12MO	AODocs Email Connector 12	$ 30.00	$ 29.33
AODocs	AODOCS-MIGRATION-TOOL-12MO	AODocs Migration Tool 12 m	$ 20,000.00	$ 19,550.00
CA Technologies	CA Agile Central Enterprise Edition	ENTP-1YR-STD	$ 420.00	$ 403.20
CA Technologies	CA Flowdock Enterprise Add-on	FDE-SUB-OD-ADD	$ 108.00	$ 103.68
CA Technologies	CA Flowdock Enterprise Standalone	FDEP-SUB-OD	$ 108.00	$ 103.68
CA Technologies	CA Agile Central HP Integration	INT-SUB-OD-HP	$ 60.00	$ 57.60
CA Technologies	CA Agile Central IBM Integration	INT-SUB-OD-IBM	$ 60.00	$ 57.60
CA Technologies	CA Agile Central Quality Manager Module	QUAL-1YR-STD	$ 120.00	$ 115.20
CA Technologies	CA Agile Central Advanced Security and Administration	RAS-SUB-OD	$ 60.00	$ 57.60
CA Technologies	CA Idea Manager Fee	RIM-SUB-FEE	$ 1,000.00	$ 960.00
CA Technologies	CA Idea Manager	RIM-SUB-OD	$ 5,000.00	$ 4,800.00
CA Technologies	CA Portfolio Manager	RPM2-SUB-OD	$ 120.00	$ 115.20
CA Technologies	CA Quality Manager Product	RQMP-1YR-STD	$ 420.00	$ 403.20
CA Technologies	CA Time Tracker Module	RTT-1YR-STD	$ 120.00	$ 115.20
CA Technologies	CA Agile Central Unlimited Edition	UE-1YR-STD	$ 588.00	$ 564.48
CA Technologies	CA API Management SaaS Portal -Partner	APIMPR990	$ 30,000.00	$ 23,520.00
CA Technologies	CA API Management SaaS Gateway add-on -Partner	APIMSA990	$ 21,600.00	$ 16,934.40
CA Technologies	CA API Management SaaS Partner	APIMSP990	$ 78,000.00	$ 61,152.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 10GB 10 Pack	APCA10990	$ 4,200.00	$ 4,200.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 20GB 10 Pack	APCA20990	$ 6,360.00	$ 6,360.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 40GB 10 Pack	APCA40990	$ 10,800.00	$ 10,800.00
CA Technologies	CA App Synthetic Monitor 1 Minute Basic 10 Pack	APCB10990	$ 7,560.00	$ 7,560.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic 50 Pack	APCB50990	$ 5,520.00	$ 5,520.00
CA Technologies	CA App Synthetic Monitor 10 Min RBM 20GB 1Pk	APCR20990	$ 4,080.00	$ 4,080.00
CA Technologies	CA App Synthetic Monitor 5 Min RBM 40GB 1Pk	APCR40990	$ 6,360.00	$ 6,360.00
CA Technologies	CA App Synthetic Monitor 15 Minute Adv 5GB 10 Pack	APMCA5990	$ 4,200.00	$ 4,200.00
CA Technologies	CA App Synthetic Monitor Adv Option	APMCMA990	$ 67,200.00	$ 67,200.00
CA Technologies	CA App Synthetic Monitor Intermediate Option	APMCMI990	$ 42,000.00	$ 42,000.00
CA Technologies	CA App Synthetic Monitor Intermediate Option	APMCMI990	$ 42,000.00	$ 42,000.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 10 pack	NCUBMF990	$ 1,740.00	$ 1,740.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 3 pack	NCUBMT990	$ 540.00	$ 540.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (10 GB) 1	NCUEAF990	$ 708.00	$ 708.00
CA Technologies	CA App Synthetic Monitor 1 Minute Basic Monitor 1	NCUEBM990	$ 1,080.00	$ 1,080.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 25 pack	NCUEBP990	$ 3,900.00	$ 3,900.00
CA Technologies	CA App Synthetic Monitor 15 Minute Advanced Monitor (5 GB) 1	NCUEMA990	$ 348.00	$ 348.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 1	NCUEMM990	$ 216.00	$ 216.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 10 pack	NCUEMP990	$ 936.00	$ 936.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 1	NCUETB990	$ 108.00	$ 108.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 3 pack	NCUETP990	$ 288.00	$ 288.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (10 GB) 10 pack	NCUMAM990	$ 6,000.00	$ 6,000.00
CA Technologies	CA App Synthetic Monitor Corporate Bundle	NCUMCB990	$ 5,940.00	$ 5,940.00
CA Technologies	CA App Synthetic Monitor Enterprise Bundle	NCUMEB990	$ 18,000.00	$ 18,000.00

CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (40 GB) 1	NCUMFA990	$ 1,800.00	$ 1,800.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (20 GB) 1	NCUMMA990	$ 1,080.00	$ 1,080.00
CA Technologies	CA App Synthetic Monitor Multi-Site Bundle	NCUMSB990	$ 1,188.00	$ 1,188.00
CA Technologies	CA Mobile App Analytics for Business Users SAAS	MBAABS565	$ 13.20	$ 11.22
CA Technologies	CA Mobile App Analytics for Consumer Users SAAS	MBAACS565	$ 0.48	$ 0.41
CA Technologies	*CA PPM SAAS Full Function User	CODSFF991	$ 720.00	$ 564.48
CA Technologies	*CA PPM SAAS Restricted User	CODSRU991	$ 360.00	$ 282.24
CA Technologies	*CA PPM SAAS VIEW ONLY USER (1000 User pack)	CODSVU991	$ 5,000.00	$ 3,920.03
CA Technologies	*CA PPM SAAS Sandbox Small Environment	CODSBX991	$ 30,000.00	$ 23,520.00
CA Technologies	*CA PPM SAAS Sandbox Near Production Environment	CODSB2991	$ 48,000.00	$ 37,632.00
DocuSign	3rd Party Solutions - Conga composer/Per Transaction - ADD ON	DS-3PS-CCT	$ 2.00	$ 1.95
DocuSign	3rd Party Solutions - Conga composer/Seat Per Year - ADD ON	DS-3PS-CCY	$ 180.00	$ 175.92
DocuSign	3rd Party Solutions - Dynamic Documents - ADD ON	DS-3PS-DD	$ 180.00	$ 175.92
DocuSign	3rd Party Solutions - eOriginal/Managed Transaction - ADD ON	DS-3PS-EMT	$ 1.00	$ 0.98
DocuSign	3rd Party Solutions - eOriginal/Transferred Transaction - ADD ON	DS-3PS-ETT	$ 5.00	$ 4.89
DocuSign	Additional - Fax Services - ADD ON	DS-AFS	$ 0.10	$ 0.10
DocuSign	DocuSign Authentication Option - ID Check - ADD ON	DS-AOID	$ 2.50	$ 2.44
DocuSign	DocuSign Authentication Option - Phone - ADD ON	DS-AOPhone	$ 0.75	$ 0.73
DocuSign	DocuSign Authentication Option - SMS - ADD ON	DS-AOSMS	$ 0.20	$ 0.20
DocuSign	Additonal - Retrieve - ADD ON	DS-AR	$ 5,000.00	$ 4,886.65
DocuSign	Customer Success Architects - Full time - SERVICE	DS-CSAF	$ 28,000.00	$ 27,365.24
DocuSign	Customer Success Architects - Half time - SERVICE	DS-CSAH	$ 18,000.00	$ 17,591.94
DocuSign	Customer Success Architects - Quarter time - SERVICE	DS-CSAQ	$ 10,000.00	$ 9,773.30
DocuSign	Docusign Digital Signatures - Express - ADD ON	DS-DSE	$ 1.50	$ 1.47
DocuSign	Docusign Digital Signatures - OpenTrust/Seat Per Year - ADD ON	DS-DSOTS	$ 144.00	$ 140.74
DocuSign	Docusign Digital Signatures - OpenTrust/Per Transaction - ADD ON	DS-DSOTT	$ 1.75	$ 1.71
DocuSign	Docusign Digital Signatures - SAFE Bio-Pharma - ADD ON	DS-DSSBP	$ 1.50	$ 1.47
DocuSign	Follow Up - TRAINING	DS-FUP	$ 295.00	$ 288.31
DocuSign	Microsoft Office 365 Quickstart Onboarding - TRAINING	DS-MO3QO	$ 295.00	$ 288.31
DocuSign	DocuSign for Office 365 Edition	DS-O3E	$ 120.00	$ 117.28
DocuSign	Powerforms - TRAINING	DS-PF	$ 295.00	$ 288.31
DocuSign	Professional Services - API Certification - SERVICE	DS-PS-APIC	$ 1,000.00	$ 977.33
DocuSign	Professional Services - Consulting - SERVICE	DS-PS-C	$ 295.00	$ 288.31
DocuSign	Professional Services - Department Strategic Assessment - SERVICE	DS-PS-DSA	$ 17,000.00	$ 16,614.61
DocuSign	Professional Services - Fast start API - SERVICE	DS-PS-FS	$ 18,000.00	$ 17,591.94
DocuSign	Professional Services - Full service API - SERVICE	DS-PS-FSAPI	$ 45,000.00	$ 43,979.85
DocuSign	Professional Services - Full service web console - SERVICE	DS-PS-FSERVWC	$ 30,000.00	$ 29,319.90
DocuSign	Professional Services - Full service Salesforce.com - SERVICE	DS-PS-FSSF	$ 35,000.00	$ 34,206.55
DocuSign	Professional Services - ProServ /Single Sign On - SERVICE	DS-PS-PSS	$ 2,500.00	$ 2,443.32
DocuSign	Professional Services - Q&A Bundle - SERVICE	DS-PS-QAB	$ 2,500.00	$ 2,443.32
DocuSign	Retrieve Training - TRAINING	DS-RT	$ 295.00	$ 288.31
DocuSign	Salesforce Admin - TRAINING	DS-SA	$ 295.00	$ 288.31
DocuSign	DocuSign System Automated Premium Edition	DS-SAPE	$ 5.00	$ 4.89
DocuSign	DocuSign for Salesforce Enterprise Editon	DS-SEE	$ 550.00	$ 537.53
DocuSign	Salesforce Installation & Configuration - TRAINING	DS-SIC	$ 295.00	$ 288.31
DocuSign	Web Console Admin - TRAINING	DS-WCA	$ 295.00	$ 288.31
DocuSign	Web Console Overview - TRAINING	DS-WCO	$ 295.00	$ 288.31
DocuSign	Web Console Template Setup - TRAINING	DS-WCTS	$ 295.00	$ 288.31
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)	DS-EE-EP	$ 121.00	$ 118.26

DocuSign	DocuSign for Salesforce Enterprise Edition Enterprise Premier (Support)- Seats- USD- Annual	12000121S-EP	$ 121.00	$ 118.26
DocuSign	DocuSign for Salesforce Enterprise Editon Enterprise Premier (Support)	DS-SEE-EP	$ 121.00	$ 118.26
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)- Seats-USD- Annual	12000111S-EP	$ 105.60	$ 103.21
DocuSign	DocuSign for Salesforce Enterprise Edition Premier (Support)- Seats- USD- Annual	12000121S-P	$ 82.50	$ 80.63
DocuSign	DocuSign for Salesforce Enterprise Editon Premier (Support)	DS-SEE-P	$ 82.50	$ 80.63
DocuSign	DocuSign for Salesforce Business Edition Enterprise Premier (Support)	12000321S-EP	$ 79.20	$ 77.40
DocuSign	DocuSign Enterprise Edition Premier (Support)- Seats-USD- Annual	12000111S-P	$ 72.00	$ 70.37
DocuSign	DocuSign for Salesforce Business Edition Premier (Support)	12000321S-P	$ 54.00	$ 52.78
DocuSign	DocuSign Enterprise Edition Premier (Support)	DS-EE-P	$ 54.00	$ 52.78
DocuSign	DocuSign for Salesforce Dynamic Documents Enterprise Premier (Support)- Seats- USD- Annual	12000232S-EP	$ 39.60	$ 38.70
DocuSign	DocuSign for Salesforce Dynamic Documents Premier (Support)- Seats- USD- Annual	12000232S-P	$ 27.00	$ 26.39
DocuSign	DocuSign for Office 365 Edition Enterprise Premier (Support)- Seat per Year	DS-O3E-EP	$ 26.40	$ 25.80
DocuSign	DocuSign for Office 365 Edition Premier (Support)- Seat per Year	DS-O3E-P	$ 18.00	$ 17.59
DocuSign	DocuSign Business Edition - SMS	200013	$ 2.00	$ 1.96
DocuSign	DocuSign for Salesforce Enterprise Edition Enterprise Premier (Support)- Envelopes- USD- Annual	12000121E-EP	$ 1.54	$ 1.52
DocuSign	DocuSign Business Edition ($/seat annually) 5+ seats	DS-BE	$ 360.00	$ 351.84
DocuSign	DocuSign for Salesforce Business Package ($/seat annually) 5+ seats	DS-SBP	$ 360.00	$ 351.84
DocuSign	DocuSign for Salesforce Enterprise Package ($/seat annually) 5+ seats	DS-SEP	$ 540.00	$ 527.76
DocuSign	DocuSign System Automated Standard Edition ($/envelope) 500 envelope allowance minimum	DS-SASE	$ 3.00	$ 2.93
DocuSign	DocuSign Enterprise Developer ($/app/year) $299/app/month	DS-ED	$ 3,588.00	$ 3,506.66
DocuSign	DocuSign Individual Developer ($/app/year) $9/app/month	DS-ID	$ 108.00	$ 105.55
DocuSign	DocuSign - Additional-Security Appliance - 40% uplift to annual Edition pricing -- Minimum 240000/year (requires product management approval)	DS-ASA	$ 240,000.00	$ 234,559.19
DocuSign	DocuSign - Additional-Connectors ($/user/year)	DS-AC	$ 144.00	$ 140.74
DocuSign	DocuSign - Professional Services -20 hr bundle Flat fee	DS-PSB	$ 5,000.00	$ 4,886.65
DocuSign	DocuSign - Strategic Value Assessments -SVA Corporate Flat fee	DS-SVA-C	$ 3,500.00	$ 3,420.65
DocuSign	DocuSign - Strategic Value Assessments -SVA Enterprise Flat fee	DS-SVA-E	$ 10,000.00	$ 9,773.30
DocuSign	DocuSign - Training-DS Transaction Rooms Broker Edition - Agent/User Training $/person	DS-TRBE-AUT	$ 295.00	$ 288.31
DocuSign	DocuSign - Training-DS Transaction Rooms Broker Edition - Admin/Account Setup $/person	DS-TRBE-AAU	$ 295.00	$ 288.31
DocuSign	DocuSign Enterprise Edition	DS-EE	$ 540.00	$ 527.76
DocuSign	Professional Services - Fast start Salesforce.com - SERVICE	DS-PS-FSS	$ 14,525.00	$ 14,195.72
DocuSign	Professional Services - Fast start web console - SERVICE	DS-PS-FSWC	$ 9,975.00	$ 9,748.87
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)- Envelopes-USD- Annual	12000111E-EP	$ 1.32	$ 1.30
DocuSign	DocuSign System Automated Premium Edition Enterprise Premier (Support)	DS-SAPE-EP	$ 1.10	$ 1.09
DocuSign	DocuSign for Salesforce Enterprise Edition Premier (Support)- Envelopes- USD- Annual	12000121E-P	$ 1.05	$ 1.04
DocuSign	DocuSign Enterprise Edition Premier (Support)- Envelopes-USD- Annual	12000111E-P	$ 0.90	$ 0.89
DocuSign	DocuSign System Automated Premium Edition Premier (Support)	DS-SAPE-P	$ 0.75	$ 0.74
DocuSign	DocuSign Business Edition Enterprise Premier (Support)- SMS	200013-EP	$ 0.44	$ 0.44
DocuSign	DocuSign for Salesforce Dynamic Documents Enterprise Premier (Support)- Envelopes- USD- Annual	12000232E-EP	$ 0.44	$ 0.44
DocuSign	DocuSign Business Edition Premier (Support)- SMS	200013-P	$ 0.30	$ 0.30
DocuSign	DocuSign for Salesforce Dynamic Documents Premier (Support)- Envelopes- USD- Annual	12000232E-P	$ 0.30	$ 0.30
FireEye	Email Threat Prevention, Platinum Support 1 Year 1-249	ETP-000249-PTM1Y	$ 58.32	$ 50.74
FireEye	Email Threat Prevention, Platinum Support 2 Year 1-249	ETP-000249-PTM2Y	$ 116.64	$ 101.48
FireEye	Email Threat Prevention, Platinum Support 3 Year 1-249	ETP-000249-PTM3Y	$ 157.46	$ 136.99
FireEye	Email Threat Prevention, Platinum Support 4 Year 1-249	ETP-000249-PTM4Y	$ 209.95	$ 182.66
FireEye	Email Threat Prevention, Platinum Support 5 Year 1-249	ETP-000249-PTM5Y	$ 262.44	$ 228.32
FireEye	Email Threat Prevention, Government US 1 Year 1-249	ETP-000249-USG1Y	$ 58.32	$ 50.74
FireEye	Email Threat Prevention, Government US 2 Year 1-249	ETP-000249-USG2Y	$ 116.64	$ 101.48
FireEye	Email Threat Prevention, Government US 3 Year 1-249	ETP-000249-USG3Y	$ 157.46	$ 136.99
FireEye	Email Threat Prevention, Government US 4 Year 1-249	ETP-000249-USG4Y	$ 209.95	$ 182.66

FireEye	Email Threat Prevention, Government US 5 Year 1-249	ETP-000249-USG5Y	$ 262.44	$ 228.32
FireEye	Email Threat Prevention, Platinum Support 1 Year 250-499	ETP-000499-PTM1Y	$ 48.15	$ 41.89
FireEye	Email Threat Prevention, Platinum Support 2 Year 250-499	ETP-000499-PTM2Y	$ 96.30	$ 83.78
FireEye	Email Threat Prevention, Platinum Support 3 Year 250-499	ETP-000499-PTM3Y	$ 130.01	$ 113.11
FireEye	Email Threat Prevention, Platinum Support 4 Year 250-499	ETP-000499-PTM4Y	$ 173.34	$ 150.81
FireEye	Email Threat Prevention, Platinum Support 5 Year 250-499	ETP-000499-PTM5Y	$ 216.68	$ 188.51
FireEye	Email Threat Prevention, Government US 1 Year 250-499	ETP-000499-USG1Y	$ 48.15	$ 41.89
FireEye	Email Threat Prevention, Government US 2 Year 250-499	ETP-000499-USG2Y	$ 96.30	$ 83.78
FireEye	Email Threat Prevention, Government US 3 Year 250-499	ETP-000499-USG3Y	$ 130.01	$ 113.11
FireEye	Email Threat Prevention, Government US 4 Year 250-499	ETP-000499-USG4Y	$ 173.34	$ 150.81
FireEye	Email Threat Prevention, Government US 5 Year 250-499	ETP-000499-USG5Y	$ 216.68	$ 188.51
FireEye	Email Threat Prevention, Platinum Support 1 Year 500-749	ETP-000749-PTM1Y	$ 41.30	$ 35.93
FireEye	Email Threat Prevention, Platinum Support 2 Year 500-749	ETP-000749-PTM2Y	$ 82.60	$ 71.86
FireEye	Email Threat Prevention, Platinum Support 3 Year 500-749	ETP-000749-PTM3Y	$ 111.51	$ 97.01
FireEye	Email Threat Prevention, Platinum Support 4 Year 500-749	ETP-000749-PTM4Y	$ 148.68	$ 129.35
FireEye	Email Threat Prevention, Platinum Support 5 Year 500-749	ETP-000749-PTM5Y	$ 185.85	$ 161.69
FireEye	Email Threat Prevention, Government US 1 Year 500-749	ETP-000749-USG1Y	$ 41.30	$ 35.93
FireEye	Email Threat Prevention, Government US 2 Year 500-749	ETP-000749-USG2Y	$ 82.60	$ 71.86
FireEye	Email Threat Prevention, Government US 3 Year 500-749	ETP-000749-USG3Y	$ 111.51	$ 97.01
FireEye	Email Threat Prevention, Government US 4 Year 500-749	ETP-000749-USG4Y	$ 148.68	$ 129.35
FireEye	Email Threat Prevention, Government US 5 Year 500-749	ETP-000749-USG5Y	$ 185.85	$ 161.69
FireEye	Email Threat Prevention, Platinum Support 1 Year 750-999	ETP-000999-PTM1Y	$ 34.69	$ 30.18
FireEye	Email Threat Prevention, Platinum Support 2 Year 750-999	ETP-000999-PTM2Y	$ 69.38	$ 60.36
FireEye	Email Threat Prevention, Platinum Support 3 Year 750-999	ETP-000999-PTM3Y	$ 93.66	$ 81.48
FireEye	Email Threat Prevention, Platinum Support 4 Year 750-999	ETP-000999-PTM4Y	$ 124.88	$ 108.65
FireEye	Email Threat Prevention, Platinum Support 5 Year 750-999	ETP-000999-PTM5Y	$ 156.11	$ 135.82
FireEye	Email Threat Prevention, Government US 1 Year 750-999	ETP-000999-USG1Y	$ 34.69	$ 30.18
FireEye	Email Threat Prevention, Government US 2 Year 750-999	ETP-000999-USG2Y	$ 69.38	$ 60.36
FireEye	Email Threat Prevention, Government US 3 Year 750-999	ETP-000999-USG3Y	$ 93.66	$ 81.48
FireEye	Email Threat Prevention, Government US 4 Year 750-999	ETP-000999-USG4Y	$ 124.88	$ 108.65
FireEye	Email Threat Prevention, Government US 5 Year 750-999	ETP-000999-USG5Y	$ 156.11	$ 135.82
FireEye	Email Threat Prevention, Platinum Support 1 Year 1,000-1999	ETP-001999-PTM1Y	$ 31.46	$ 27.37
FireEye	Email Threat Prevention, Platinum Support 2 Year 1,000-1999	ETP-001999-PTM2Y	$ 62.92	$ 54.74
FireEye	Email Threat Prevention, Platinum Support 3 Year 1,000-1999	ETP-001999-PTM3Y	$ 84.94	$ 73.90
FireEye	Email Threat Prevention, Platinum Support 4 Year 1,000-1999	ETP-001999-PTM4Y	$ 113.26	$ 98.54
FireEye	Email Threat Prevention, Platinum Support 5 Year 1,000-1999	ETP-001999-PTM5Y	$ 141.57	$ 123.17
FireEye	Email Threat Prevention, Government US 1 Year 1,000-1999	ETP-001999-USG1Y	$ 31.46	$ 27.37
FireEye	Email Threat Prevention, Government US 2 Year 1,000-1999	ETP-001999-USG2Y	$ 62.92	$ 54.74
FireEye	Email Threat Prevention, Government US 3 Year 1,000-1999	ETP-001999-USG3Y	$ 84.94	$ 73.90
FireEye	Email Threat Prevention, Government US 4 Year 1,000-1999	ETP-001999-USG4Y	$ 113.26	$ 98.54
FireEye	Email Threat Prevention, Government US 5 Year 1,000-1999	ETP-001999-USG5Y	$ 141.57	$ 123.17
FireEye	Email Threat Prevention, Platinum Support 1 Year 2,000-4999	ETP-004999-PTM1Y	$ 28.64	$ 24.92
FireEye	Email Threat Prevention, Platinum Support 2 Year 2,000-4999	ETP-004999-PTM2Y	$ 57.28	$ 49.83
FireEye	Email Threat Prevention, Platinum Support 3 Year 2,000-4999	ETP-004999-PTM3Y	$ 77.33	$ 67.28
FireEye	Email Threat Prevention, Platinum Support 4 Year 2,000-4999	ETP-004999-PTM4Y	$ 103.10	$ 89.70
FireEye	Email Threat Prevention, Platinum Support 5 Year 2,000-4999	ETP-004999-PTM5Y	$ 128.88	$ 112.13
FireEye	Email Threat Prevention, Government US 1 Year 2,000-4999	ETP-004999-USG1Y	$ 28.64	$ 24.92
FireEye	Email Threat Prevention, Government US 2 Year 2,000-4999	ETP-004999-USG2Y	$ 57.28	$ 49.83
FireEye	Email Threat Prevention, Government US 3 Year 2,000-4999	ETP-004999-USG3Y	$ 77.33	$ 67.28

FireEye	Email Threat Prevention, Government US 4 Year 2,000-4999	ETP-004999-USG4Y	$ 103.10	$ 89.70
FireEye	Email Threat Prevention, Government US 5 Year 2,000-4999	ETP-004999-USG5Y	$ 128.88	$ 112.13
FireEye	Email Threat Prevention, Platinum Support 1 Year 5,000-9999	ETP-009999-PTM1Y	$ 25.51	$ 22.19
FireEye	Email Threat Prevention, Platinum Support 2 Year 5,000-9999	ETP-009999-PTM2Y	$ 51.02	$ 44.39
FireEye	Email Threat Prevention, Platinum Support 3 Year 5,000-9999	ETP-009999-PTM3Y	$ 68.88	$ 59.93
FireEye	Email Threat Prevention, Platinum Support 4 Year 5,000-9999	ETP-009999-PTM4Y	$ 91.84	$ 79.90
FireEye	Email Threat Prevention, Platinum Support 5 Year 5,000-9999	ETP-009999-PTM5Y	$ 114.80	$ 99.88
FireEye	Email Threat Prevention, Government US 1 Year 5,000-9999	ETP-009999-USG1Y	$ 25.51	$ 22.19
FireEye	Email Threat Prevention, Government US 2 Year 5,000-9999	ETP-009999-USG2Y	$ 51.02	$ 44.39
FireEye	Email Threat Prevention, Government US 3 Year 5,000-9999	ETP-009999-USG3Y	$ 68.88	$ 59.93
FireEye	Email Threat Prevention, Government US 4 Year 5,000-9999	ETP-009999-USG4Y	$ 91.84	$ 79.90
FireEye	Email Threat Prevention, Government US 5 Year 5,000-9999	ETP-009999-USG5Y	$ 114.80	$ 99.88
FireEye	Email Threat Prevention, Platinum Support 1 Year 10,000-19999	ETP-019999-PTM1Y	$ 22.02	$ 19.16
FireEye	Email Threat Prevention, Platinum Support 2 Year 10,000-19999	ETP-019999-PTM2Y	$ 44.04	$ 38.31
FireEye	Email Threat Prevention, Platinum Support 3 Year 10,000-19999	ETP-019999-PTM3Y	$ 59.45	$ 51.72
FireEye	Email Threat Prevention, Platinum Support 4 Year 10,000-19999	ETP-019999-PTM4Y	$ 79.27	$ 68.96
FireEye	Email Threat Prevention, Platinum Support 5 Year 10,000-19999	ETP-019999-PTM5Y	$ 99.09	$ 86.21
FireEye	Email Threat Prevention, Government US 1 Year 10,000-19999	ETP-019999-USG1Y	$ 22.02	$ 19.16
FireEye	Email Threat Prevention, Government US 2 Year 10,000-19999	ETP-019999-USG2Y	$ 44.04	$ 38.31
FireEye	Email Threat Prevention, Government US 3 Year 10,000-19999	ETP-019999-USG3Y	$ 59.45	$ 51.72
FireEye	Email Threat Prevention, Government US 4 Year 10,000-19999	ETP-019999-USG4Y	$ 79.27	$ 68.96
FireEye	Email Threat Prevention, Government US 5 Year 10,000-19999	ETP-019999-USG5Y	$ 99.09	$ 86.21
FireEye	Email Threat Prevention, Platinum Support 1 Year 20,000-49999	ETP-049999-PTM1Y	$ 20.76	$ 18.06
FireEye	Email Threat Prevention, Platinum Support 2 Year 20,000-49999	ETP-049999-PTM2Y	$ 41.52	$ 36.12
FireEye	Email Threat Prevention, Platinum Support 3 Year 20,000-49999	ETP-049999-PTM3Y	$ 56.05	$ 48.76
FireEye	Email Threat Prevention, Platinum Support 4 Year 20,000-49999	ETP-049999-PTM4Y	$ 74.74	$ 65.02
FireEye	Email Threat Prevention, Platinum Support 5 Year 20,000-49999	ETP-049999-PTM5Y	$ 93.42	$ 81.28
FireEye	Email Threat Prevention, Government US 1 Year 20,000-49999	ETP-049999-USG1Y	$ 20.76	$ 18.06
FireEye	Email Threat Prevention, Government US 2 Year 20,000-49999	ETP-049999-USG2Y	$ 41.52	$ 36.12
FireEye	Email Threat Prevention, Government US 3 Year 20,000-49999	ETP-049999-USG3Y	$ 56.05	$ 48.76
FireEye	Email Threat Prevention, Government US 4 Year 20,000-49999	ETP-049999-USG4Y	$ 74.74	$ 65.02
FireEye	Email Threat Prevention, Government US 5 Year 20,000-49999	ETP-049999-USG5Y	$ 93.42	$ 81.28
FireEye	Email Threat Prevention, Platinum Support 1 Year 50,000-74999	ETP-074999-PTM1Y	$ 18.75	$ 16.31
FireEye	Email Threat Prevention, Platinum Support 2 Year 50,000-74999	ETP-074999-PTM2Y	$ 37.50	$ 32.63
FireEye	Email Threat Prevention, Platinum Support 3 Year 50,000-74999	ETP-074999-PTM3Y	$ 50.63	$ 44.05
FireEye	Email Threat Prevention, Platinum Support 4 Year 50,000-74999	ETP-074999-PTM4Y	$ 67.50	$ 58.73
FireEye	Email Threat Prevention, Platinum Support 5 Year 50,000-74999	ETP-074999-PTM5Y	$ 84.38	$ 73.41
FireEye	Email Threat Prevention, Government US 1 Year 50,000-74999	ETP-074999-USG1Y	$ 18.75	$ 16.31
FireEye	Email Threat Prevention, Government US 2 Year 50,000-74999	ETP-074999-USG2Y	$ 37.50	$ 32.63
FireEye	Email Threat Prevention, Government US 3 Year 50,000-74999	ETP-074999-USG3Y	$ 50.63	$ 44.05
FireEye	Email Threat Prevention, Government US 4 Year 50,000-74999	ETP-074999-USG4Y	$ 67.50	$ 58.73
FireEye	Email Threat Prevention, Government US 5 Year 50,000-74999	ETP-074999-USG5Y	$ 84.38	$ 73.41
FireEye	Email Threat Prevention, Platinum Support 1 Year 75,000-99999	ETP-099999-PTM1Y	$ 16.22	$ 14.11
FireEye	Email Threat Prevention, Platinum Support 2 Year 75,000-99999	ETP-099999-PTM2Y	$ 32.44	$ 28.22
FireEye	Email Threat Prevention, Platinum Support 3 Year 75,000-99999	ETP-099999-PTM3Y	$ 43.79	$ 38.10
FireEye	Email Threat Prevention, Platinum Support 4 Year 75,000-99999	ETP-099999-PTM4Y	$ 58.39	$ 50.80
FireEye	Email Threat Prevention, Platinum Support 5 Year 75,000-99999	ETP-099999-PTM5Y	$ 72.99	$ 63.50
FireEye	Email Threat Prevention, Government US 1 Year 75,000-99999	ETP-099999-USG1Y	$ 16.22	$ 14.11
FireEye	Email Threat Prevention, Government US 2 Year 75,000-99999	ETP-099999-USG2Y	$ 32.44	$ 28.22

FireEye	Email Threat Prevention, Government US 3 Year 75,000-99999	ETP-099999-USG3Y	$ 43.79	$ 38.10
FireEye	Email Threat Prevention, Government US 4 Year 75,000-99999	ETP-099999-USG4Y	$ 58.39	$ 50.80
FireEye	Email Threat Prevention, Government US 5 Year 75,000-99999	ETP-099999-USG5Y	$ 72.99	$ 63.50
FireEye	Email Threat Prevention, Platinum Support 1 Year 100,000-199999	ETP-199999-PTM1Y	$ 14.26	$ 12.41
FireEye	Email Threat Prevention, Platinum Support 2 Year 100,000-199999	ETP-199999-PTM2Y	$ 28.52	$ 24.81
FireEye	Email Threat Prevention, Platinum Support 3 Year 100,000-199999	ETP-199999-PTM3Y	$ 38.50	$ 33.50
FireEye	Email Threat Prevention, Platinum Support 4 Year 100,000-199999	ETP-199999-PTM4Y	$ 51.34	$ 44.67
FireEye	Email Threat Prevention, Platinum Support 5 Year 100,000-199999	ETP-199999-PTM5Y	$ 64.17	$ 55.83
FireEye	Email Threat Prevention, Government US 1 Year 100,000-199999	ETP-199999-USG1Y	$ 14.26	$ 12.41
FireEye	Email Threat Prevention, Government US 2 Year 100,000-199999	ETP-199999-USG2Y	$ 28.52	$ 24.81
FireEye	Email Threat Prevention, Government US 3 Year 100,000-199999	ETP-199999-USG3Y	$ 38.50	$ 33.50
FireEye	Email Threat Prevention, Government US 4 Year 100,000-199999	ETP-199999-USG4Y	$ 51.34	$ 44.67
FireEye	Email Threat Prevention, Government US 5 Year 100,000-199999	ETP-199999-USG5Y	$ 64.17	$ 55.83
FireEye	Email Threat Prevention, Platinum Support 1 Year 200,000+	ETP-200000+PTM1Y	$ 13.46	$ 11.71
FireEye	Email Threat Prevention, Platinum Support 2 Year 200,000+	ETP-200000+PTM2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention, Platinum Support 3 Year 200,000+	ETP-200000+PTM3Y	$ 36.34	$ 31.62
FireEye	Email Threat Prevention, Platinum Support 4 Year 200,000+	ETP-200000+PTM4Y	$ 48.46	$ 42.16
FireEye	Email Threat Prevention, Platinum Support 5 Year 200,000+	ETP-200000+PTM5Y	$ 60.57	$ 52.70
FireEye	Email Threat Prevention, Government US 1 Year 200,000+	ETP-200000+USG1Y	$ 13.46	$ 11.71
FireEye	Email Threat Prevention, Government US 2 Year 200,000+	ETP-200000+USG2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention, Government US 3 Year 200,000+	ETP-200000+USG3Y	$ 36.34	$ 31.62
FireEye	Email Threat Prevention, Government US 4 Year 200,000+	ETP-200000+USG4Y	$ 48.46	$ 42.16
FireEye	Email Threat Prevention, Government US 5 Year 200,000+	ETP-200000+USG5Y	$ 60.57	$ 52.70
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1-249	ETP-A-000249-CAG1Y	$ 71.95	$ 62.60
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1-249	ETP-A-000249-CAG2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1-249	ETP-A-000249-CAG3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1-249	ETP-A-000249-CAG4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1-249	ETP-A-000249-CAG5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1-249	ETP-A-000249-CAP1Y	$ 75.00	$ 65.25
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1-249	ETP-A-000249-CAP2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1-249	ETP-A-000249-CAP3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1-249	ETP-A-000249-CAP4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1-249	ETP-A-000249-CAP5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1-249	ETP-A-000249-PPL1Y	$ 13.62	$ 11.85
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1-249	ETP-A-000249-PPL2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1-249	ETP-A-000249-PPL3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1-249	ETP-A-000249-PPL4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1-249	ETP-A-000249-PPL5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1-249	ETP-A-000249-PTM1Y	$ 26.24	$ 22.83
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1-249	ETP-A-000249-PTM2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1-249	ETP-A-000249-PTM3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1-249	ETP-A-000249-PTM4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1-249	ETP-A-000249-PTM5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 1-249	ETP-A-000249-USG1Y	$ 71.95	$ 62.60
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 1-249	ETP-A-000249-USG2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 1-249	ETP-A-000249-USG3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 1-249	ETP-A-000249-USG4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 1-249	ETP-A-000249-USG5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1-249	ETP-A-000249-USP1Y	$ 75.00	$ 65.25

FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1-249	ETP-A-000249-USP2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1-249	ETP-A-000249-USP3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1-249	ETP-A-000249-USP4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1-249	ETP-A-000249-USP5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 250-499	ETP-A-000499-CAG1Y	$ 35.96	$ 31.29
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 250-499	ETP-A-000499-CAG2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 250-499	ETP-A-000499-CAG3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 250-499	ETP-A-000499-CAG4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 250-499	ETP-A-000499-CAG5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 250-499	ETP-A-000499-CAP1Y	$ 37.48	$ 32.61
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 250-499	ETP-A-000499-CAP2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 250-499	ETP-A-000499-CAP3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 250-499	ETP-A-000499-CAP4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 250-499	ETP-A-000499-CAP5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 250-499	ETP-A-000499-PPL1Y	$ 11.26	$ 9.80
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 250-499	ETP-A-000499-PPL2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 250-499	ETP-A-000499-PPL3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 250-499	ETP-A-000499-PPL4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 250-499	ETP-A-000499-PPL5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 250-499	ETP-A-000499-PTM1Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 250-499	ETP-A-000499-PTM2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 250-499	ETP-A-000499-PTM3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 250-499	ETP-A-000499-PTM4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 250-499	ETP-A-000499-PTM5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 250-499	ETP-A-000499-USG1Y	$ 35.96	$ 31.29
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 250-499	ETP-A-000499-USG2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 250-499	ETP-A-000499-USG3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 250-499	ETP-A-000499-USG4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 250-499	ETP-A-000499-USG5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 250-499	ETP-A-000499-USP1Y	$ 37.48	$ 32.61
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 250-499	ETP-A-000499-USP2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 250-499	ETP-A-000499-USP3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 250-499	ETP-A-000499-USP4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 250-499	ETP-A-000499-USP5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 500-749	ETP-A-000749-CAG1Y	$ 29.76	$ 25.89
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 500-749	ETP-A-000749-CAG2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 500-749	ETP-A-000749-CAG3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 500-749	ETP-A-000749-CAG4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 500-749	ETP-A-000749-CAG5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 500-749	ETP-A-000749-CAP1Y	$ 31.02	$ 26.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 500-749	ETP-A-000749-CAP2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 500-749	ETP-A-000749-CAP3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 500-749	ETP-A-000749-CAP4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 500-749	ETP-A-000749-CAP5Y	$ 139.59	$ 121.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 500-749	ETP-A-000749-PPL1Y	$ 9.66	$ 8.40
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 500-749	ETP-A-000749-PPL2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 500-749	ETP-A-000749-PPL3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 500-749	ETP-A-000749-PPL4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 500-749	ETP-A-000749-PPL5Y	$ 139.59	$ 121.44

FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 500-749	ETP-A-000749-PTM1Y	$ 18.59	$ 16.17
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 500-749	ETP-A-000749-PTM2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 500-749	ETP-A-000749-PTM3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 500-749	ETP-A-000749-PTM4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 500-749	ETP-A-000749-PTM5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 500-749	ETP-A-000749-USG1Y	$ 29.76	$ 25.89
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 500-749	ETP-A-000749-USG2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 500-749	ETP-A-000749-USG3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 500-749	ETP-A-000749-USG4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 500-749	ETP-A-000749-USG5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 500-749	ETP-A-000749-USP1Y	$ 31.02	$ 26.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 500-749	ETP-A-000749-USP2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 500-749	ETP-A-000749-USP3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 500-749	ETP-A-000749-USP4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 500-749	ETP-A-000749-USP5Y	$ 139.59	$ 121.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 750-999	ETP-A-000999-CAG1Y	$ 29.03	$ 25.26
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 750-999	ETP-A-000999-CAG2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 750-999	ETP-A-000999-CAG3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 750-999	ETP-A-000999-CAG4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 750-999	ETP-A-000999-CAG5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 750-999	ETP-A-000999-CAP1Y	$ 30.26	$ 26.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 750-999	ETP-A-000999-CAP2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 750-999	ETP-A-000999-CAP3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 750-999	ETP-A-000999-CAP4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 750-999	ETP-A-000999-CAP5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 750-999	ETP-A-000999-PPL1Y	$ 8.11	$ 7.06
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 750-999	ETP-A-000999-PPL2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 750-999	ETP-A-000999-PPL3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 750-999	ETP-A-000999-PPL4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 750-999	ETP-A-000999-PPL5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 750-999	ETP-A-000999-PTM1Y	$ 15.61	$ 13.58
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 750-999	ETP-A-000999-PTM2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 750-999	ETP-A-000999-PTM3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 750-999	ETP-A-000999-PTM4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 750-999	ETP-A-000999-PTM5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 750-999	ETP-A-000999-USG1Y	$ 29.03	$ 25.26
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 750-999	ETP-A-000999-USG2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 750-999	ETP-A-000999-USG3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 750-999	ETP-A-000999-USG4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 750-999	ETP-A-000999-USG5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 750-999	ETP-A-000999-USP1Y	$ 30.26	$ 26.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 750-999	ETP-A-000999-USP2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 750-999	ETP-A-000999-USP3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 750-999	ETP-A-000999-USP4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 750-999	ETP-A-000999-USP5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1,000-1999	ETP-A-001999-CAG1Y	$ 22.35	$ 19.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1,000-1999	ETP-A-001999-CAG2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1,000-1999	ETP-A-001999-CAG3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1,000-1999	ETP-A-001999-CAG4Y	$ 80.46	$ 70.00

FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1,000-1999	ETP-A-001999-CAG5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1,000-1999	ETP-A-001999-CAP1Y	$ 23.29	$ 20.26
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1,000-1999	ETP-A-001999-CAP2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1,000-1999	ETP-A-001999-CAP3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1,000-1999	ETP-A-001999-CAP4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1,000-1999	ETP-A-001999-CAP5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1,000-1999	ETP-A-001999-PPL1Y	$ 7.35	$ 6.39
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1,000-1999	ETP-A-001999-PPL2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1,000-1999	ETP-A-001999-PPL3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1,000-1999	ETP-A-001999-PPL4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1,000-1999	ETP-A-001999-PPL5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1,000-1999	ETP-A-001999-PTM1Y	$ 14.16	$ 12.32
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1,000-1999	ETP-A-001999-PTM2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1,000-1999	ETP-A-001999-PTM3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1,000-1999	ETP-A-001999-PTM4Y	$ 80.46	$ 70.00
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1,000-1999	ETP-A-001999-PTM5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 1,000-1999	ETP-A-001999-USG1Y	$ 22.35	$ 19.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 1,000-1999	ETP-A-001999-USG2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 1,000-1999	ETP-A-001999-USG3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 1,000-1999	ETP-A-001999-USG4Y	$ 80.46	$ 70.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 1,000-1999	ETP-A-001999-USG5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-A-001999-USP1Y	$ 23.29	$ 20.26
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-A-001999-USP2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-A-001999-USP3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-A-001999-USP4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-A-001999-USP5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 2,000-4999	ETP-A-004999-CAG1Y	$ 16.67	$ 14.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 2,000-4999	ETP-A-004999-CAG2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 2,000-4999	ETP-A-004999-CAG3Y	$ 45.01	$ 39.16
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 2,000-4999	ETP-A-004999-CAG4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 2,000-4999	ETP-A-004999-CAG5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 2,000-4999	ETP-A-004999-CAP1Y	$ 17.38	$ 15.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 2,000-4999	ETP-A-004999-CAP2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 2,000-4999	ETP-A-004999-CAP3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 2,000-4999	ETP-A-004999-CAP4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 2,000-4999	ETP-A-004999-CAP5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 2,000-4999	ETP-A-004999-PPL1Y	$ 6.70	$ 5.83
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 2,000-4999	ETP-A-004999-PPL2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 2,000-4999	ETP-A-004999-PPL3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 2,000-4999	ETP-A-004999-PPL4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 2,000-4999	ETP-A-004999-PPL5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 2,000-4999	ETP-A-004999-PTM1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 2,000-4999	ETP-A-004999-PTM2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 2,000-4999	ETP-A-004999-PTM3Y	$ 45.01	$ 39.16
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 2,000-4999	ETP-A-004999-PTM4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 2,000-4999	ETP-A-004999-PTM5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 2,000-4999	ETP-A-004999-USG1Y	$ 16.67	$ 14.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 2,000-4999	ETP-A-004999-USG2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 2,000-4999	ETP-A-004999-USG3Y	$ 45.01	$ 39.16

FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 2,000-4999	ETP-A-004999-USG4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 2,000-4999	ETP-A-004999-USG5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-A-004999-USP1Y	$ 17.38	$ 15.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-A-004999-USP2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-A-004999-USP3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-A-004999-USP4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-A-004999-USP5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 5,000-9999	ETP-A-009999-CAG1Y	$ 14.75	$ 12.83
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 5,000-9999	ETP-A-009999-CAG2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 5,000-9999	ETP-A-009999-CAG3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 5,000-9999	ETP-A-009999-CAG4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 5,000-9999	ETP-A-009999-CAG5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 5,000-9999	ETP-A-009999-CAP1Y	$ 15.37	$ 13.37
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 5,000-9999	ETP-A-009999-CAP2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 5,000-9999	ETP-A-009999-CAP3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 5,000-9999	ETP-A-009999-CAP4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 5,000-9999	ETP-A-009999-CAP5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 5,000-9999	ETP-A-009999-PPL1Y	$ 8.29	$ 7.21
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 5,000-9999	ETP-A-009999-PPL2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 5,000-9999	ETP-A-009999-PPL3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 5,000-9999	ETP-A-009999-PPL4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 5,000-9999	ETP-A-009999-PPL5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 5,000-9999	ETP-A-009999-PTM1Y	$ 13.71	$ 11.93
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 5,000-9999	ETP-A-009999-PTM2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 5,000-9999	ETP-A-009999-PTM3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 5,000-9999	ETP-A-009999-PTM4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 5,000-9999	ETP-A-009999-PTM5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 5,000-9999	ETP-A-009999-USG1Y	$ 14.75	$ 12.83
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 5,000-9999	ETP-A-009999-USG2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 5,000-9999	ETP-A-009999-USG3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 5,000-9999	ETP-A-009999-USG4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 5,000-9999	ETP-A-009999-USG5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-A-009999-USP1Y	$ 15.37	$ 13.37
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-A-009999-USP2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-A-009999-USP3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-A-009999-USP4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-A-009999-USP5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 10,000-19999	ETP-A-019999-CAG1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 10,000-19999	ETP-A-019999-CAG2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 10,000-19999	ETP-A-019999-CAG3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 10,000-19999	ETP-A-019999-CAG4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 10,000-19999	ETP-A-019999-CAG5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 10,000-19999	ETP-A-019999-CAP1Y	$ 13.44	$ 11.69
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 10,000-19999	ETP-A-019999-CAP2Y	$ 25.13	$ 21.86
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 10,000-19999	ETP-A-019999-CAP3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 10,000-19999	ETP-A-019999-CAP4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 10,000-19999	ETP-A-019999-CAP5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 10,000-19999	ETP-A-019999-PPL1Y	$ 6.07	$ 5.28
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 10,000-19999	ETP-A-019999-PPL2Y	$ 25.13	$ 21.86

FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 10,000-19999	ETP-A-019999-PPL3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 10,000-19999	ETP-A-019999-PPL4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 10,000-19999	ETP-A-019999-PPL5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 10,000-19999	ETP-A-019999-PTM1Y	$ 10.79	$ 9.39
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 10,000-19999	ETP-A-019999-PTM2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 10,000-19999	ETP-A-019999-PTM3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 10,000-19999	ETP-A-019999-PTM4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 10,000-19999	ETP-A-019999-PTM5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 10,000-19999	ETP-A-019999-USG1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 10,000-19999	ETP-A-019999-USG2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 10,000-19999	ETP-A-019999-USG3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 10,000-19999	ETP-A-019999-USG4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 10,000-19999	ETP-A-019999-USG5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-A-019999-USP1Y	$ 13.44	$ 11.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-A-019999-USP2Y	$ 25.13	$ 21.86
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-A-019999-USP3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-A-019999-USP4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-A-019999-USP5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 20,000-49999	ETP-A-049999-CAG1Y	$ 11.55	$ 10.05
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 20,000-49999	ETP-A-049999-CAG2Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 20,000-49999	ETP-A-049999-CAG3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 20,000-49999	ETP-A-049999-CAG4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 20,000-49999	ETP-A-049999-CAG5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 20,000-49999	ETP-A-049999-CAP1Y	$ 12.04	$ 10.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 20,000-49999	ETP-A-049999-CAP2Y	$ 22.59	$ 19.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 20,000-49999	ETP-A-049999-CAP3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 20,000-49999	ETP-A-049999-CAP4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 20,000-49999	ETP-A-049999-CAP5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 20,000-49999	ETP-A-049999-PPL1Y	$ 4.85	$ 4.22
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 20,000-49999	ETP-A-049999-PPL2Y	$ 22.50	$ 19.58
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 20,000-49999	ETP-A-049999-PPL3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 20,000-49999	ETP-A-049999-PPL4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 20,000-49999	ETP-A-049999-PPL5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 20,000-49999	ETP-A-049999-PTM1Y	$ 9.34	$ 8.13
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 20,000-49999	ETP-A-049999-PTM2Y	$ 21.59	$ 18.78
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 20,000-49999	ETP-A-049999-PTM3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 20,000-49999	ETP-A-049999-PTM4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 20,000-49999	ETP-A-049999-PTM5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 20,000-49999	ETP-A-049999-USG1Y	$ 11.55	$ 10.05
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 20,000-49999	ETP-A-049999-USG2Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 20,000-49999	ETP-A-049999-USG3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 20,000-49999	ETP-A-049999-USG4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 20,000-49999	ETP-A-049999-USG5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-A-049999-USP1Y	$ 12.04	$ 10.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-A-049999-USP2Y	$ 22.59	$ 19.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-A-049999-USP3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-A-049999-USP4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-A-049999-USP5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 50,000-74999	ETP-A-074999-CAG1Y	$ 11.84	$ 10.30

FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 50,000-74999	ETP-A-074999-CAG2Y	$ 22.18	$ 19.30
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 50,000-74999	ETP-A-074999-CAG3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 50,000-74999	ETP-A-074999-CAG4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 50,000-74999	ETP-A-074999-CAG5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 50,000-74999	ETP-A-074999-CAP1Y	$ 12.34	$ 10.74
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 50,000-74999	ETP-A-074999-CAP2Y	$ 23.13	$ 20.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 50,000-74999	ETP-A-074999-CAP3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 50,000-74999	ETP-A-074999-CAP4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 50,000-74999	ETP-A-074999-CAP5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 50,000-74999	ETP-A-074999-PPL1Y	$ 4.76	$ 4.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 50,000-74999	ETP-A-074999-PPL2Y	$ 23.06	$ 20.06
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 50,000-74999	ETP-A-074999-PPL3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 50,000-74999	ETP-A-074999-PPL4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 50,000-74999	ETP-A-074999-PPL5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 50,000-74999	ETP-A-074999-PTM1Y	$ 8.80	$ 7.66
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 50,000-74999	ETP-A-074999-PTM2Y	$ 22.14	$ 19.26
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 50,000-74999	ETP-A-074999-PTM3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 50,000-74999	ETP-A-074999-PTM4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 50,000-74999	ETP-A-074999-PTM5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 50,000-74999	ETP-A-074999-USG1Y	$ 11.84	$ 10.30
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 50,000-74999	ETP-A-074999-USG2Y	$ 22.18	$ 19.30
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 50,000-74999	ETP-A-074999-USG3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 50,000-74999	ETP-A-074999-USG4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 50,000-74999	ETP-A-074999-USG5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-A-074999-USP1Y	$ 12.34	$ 10.74
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-A-074999-USP2Y	$ 23.13	$ 20.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-A-074999-USP3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-A-074999-USP4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-A-074999-USP5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 75,000-99999	ETP-A-099999-CAG1Y	$ 12.39	$ 10.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 75,000-99999	ETP-A-099999-CAG2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 75,000-99999	ETP-A-099999-CAG3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 75,000-99999	ETP-A-099999-CAG4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 75,000-99999	ETP-A-099999-CAG5Y	$ 55.76	$ 48.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 75,000-99999	ETP-A-099999-CAP1Y	$ 12.91	$ 11.23
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 75,000-99999	ETP-A-099999-CAP2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 75,000-99999	ETP-A-099999-CAP3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 75,000-99999	ETP-A-099999-CAP4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 75,000-99999	ETP-A-099999-CAP5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 75,000-99999	ETP-A-099999-PPL1Y	$ 4.76	$ 4.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 75,000-99999	ETP-A-099999-PPL2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 75,000-99999	ETP-A-099999-PPL3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 75,000-99999	ETP-A-099999-PPL4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 75,000-99999	ETP-A-099999-PPL5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 75,000-99999	ETP-A-099999-PTM1Y	$ 8.22	$ 7.15
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 75,000-99999	ETP-A-099999-PTM2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 75,000-99999	ETP-A-099999-PTM3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 75,000-99999	ETP-A-099999-PTM4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 75,000-99999	ETP-A-099999-PTM5Y	$ 55.76	$ 48.51

FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 75,000-99999	ETP-A-099999-USG1Y	$ 12.39	$ 10.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 75,000-99999	ETP-A-099999-USG2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 75,000-99999	ETP-A-099999-USG3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 75,000-99999	ETP-A-099999-USG4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 75,000-99999	ETP-A-099999-USG5Y	$ 55.76	$ 48.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-A-099999-USP1Y	$ 12.91	$ 11.23
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-A-099999-USP2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-A-099999-USP3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-A-099999-USP4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-A-099999-USP5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 100,000-199999	ETP-A-199999-CAG1Y	$ 10.78	$ 9.38
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 100,000-199999	ETP-A-199999-CAG2Y	$ 20.15	$ 17.53
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 100,000-199999	ETP-A-199999-CAG3Y	$ 29.11	$ 25.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 100,000-199999	ETP-A-199999-CAG4Y	$ 38.81	$ 33.76
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 100,000-199999	ETP-A-199999-CAG5Y	$ 48.51	$ 42.20
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 100,000-199999	ETP-A-199999-CAP1Y	$ 11.23	$ 9.77
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 100,000-199999	ETP-A-199999-CAP2Y	$ 21.01	$ 18.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 100,000-199999	ETP-A-199999-CAP3Y	$ 30.32	$ 26.38
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 100,000-199999	ETP-A-199999-CAP4Y	$ 40.43	$ 35.17
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 100,000-199999	ETP-A-199999-CAP5Y	$ 50.54	$ 43.97
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 100,000-199999	ETP-A-199999-PPL1Y	$ 3.50	$ 3.05
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 100,000-199999	ETP-A-199999-PPL2Y	$ 21.09	$ 18.35
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 100,000-199999	ETP-A-199999-PPL3Y	$ 30.48	$ 26.52
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 100,000-199999	ETP-A-199999-PPL4Y	$ 40.64	$ 35.36
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 100,000-199999	ETP-A-199999-PPL5Y	$ 50.81	$ 44.20
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 100,000-199999	ETP-A-199999-PTM1Y	$ 6.58	$ 5.72
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 100,000-199999	ETP-A-199999-PTM2Y	$ 20.25	$ 17.62
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 100,000-199999	ETP-A-199999-PTM3Y	$ 29.24	$ 25.44
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 100,000-199999	ETP-A-199999-PTM4Y	$ 38.99	$ 33.92
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 100,000-199999	ETP-A-199999-PTM5Y	$ 48.74	$ 42.40
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 100,000-199999	ETP-A-199999-USG1Y	$ 10.78	$ 9.38
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 100,000-199999	ETP-A-199999-USG2Y	$ 20.15	$ 17.53
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 100,000-199999	ETP-A-199999-USG3Y	$ 29.11	$ 25.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 100,000-199999	ETP-A-199999-USG4Y	$ 38.81	$ 33.76
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 100,000-199999	ETP-A-199999-USG5Y	$ 48.51	$ 42.20
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-A-199999-USP1Y	$ 11.23	$ 9.77
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-A-199999-USP2Y	$ 21.01	$ 18.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-A-199999-USP3Y	$ 30.32	$ 26.38
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-A-199999-USP4Y	$ 40.43	$ 35.17
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-A-199999-USP5Y	$ 50.54	$ 43.97
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 200,000+	ETP-A-200000+CAG1Y	$ 10.42	$ 9.07
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 200,000+	ETP-A-200000+CAG2Y	$ 19.49	$ 16.96
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 200,000+	ETP-A-200000+CAG3Y	$ 28.13	$ 24.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 200,000+	ETP-A-200000+CAG4Y	$ 37.51	$ 32.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 200,000+	ETP-A-200000+CAG5Y	$ 46.89	$ 40.79
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 200,000+	ETP-A-200000+CAP1Y	$ 10.86	$ 9.45
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 200,000+	ETP-A-200000+CAP2Y	$ 20.30	$ 17.66
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 200,000+	ETP-A-200000+CAP3Y	$ 29.32	$ 25.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 200,000+	ETP-A-200000+CAP4Y	$ 39.10	$ 34.02

FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 200,000+	ETP-A-200000+CAP5Y	$ 48.87	$ 42.52
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 200,000+	ETP-A-200000+PPL1Y	$ 3.13	$ 2.72
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 200,000+	ETP-A-200000+PPL2Y	$ 20.32	$ 17.68
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 200,000+	ETP-A-200000+PPL3Y	$ 29.38	$ 25.56
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 200,000+	ETP-A-200000+PPL4Y	$ 39.17	$ 34.08
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 200,000+	ETP-A-200000+PPL5Y	$ 48.96	$ 42.60
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 200,000+	ETP-A-200000+PTM1Y	$ 6.04	$ 5.25
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 200,000+	ETP-A-200000+PTM2Y	$ 19.51	$ 16.97
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 200,000+	ETP-A-200000+PTM3Y	$ 28.16	$ 24.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 200,000+	ETP-A-200000+PTM4Y	$ 37.55	$ 32.67
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 200,000+	ETP-A-200000+PTM5Y	$ 46.94	$ 40.84
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 200,000+	ETP-A-200000+USG1Y	$ 10.42	$ 9.07
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 200,000+	ETP-A-200000+USG2Y	$ 19.49	$ 16.96
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 200,000+	ETP-A-200000+USG3Y	$ 28.13	$ 24.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 200,000+	ETP-A-200000+USG4Y	$ 37.51	$ 32.63
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 200,000+	ETP-A-200000+USG5Y	$ 46.89	$ 40.79
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 200,000+	ETP-A-200000+USP1Y	$ 10.86	$ 9.45
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 200,000+	ETP-A-200000+USP2Y	$ 20.30	$ 17.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 200,000+	ETP-A-200000+USP3Y	$ 29.32	$ 25.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 200,000+	ETP-A-200000+USP4Y	$ 39.10	$ 34.02
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 200,000+	ETP-A-200000+USP5Y	$ 48.87	$ 42.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1-249	ETP-C-000249-CAG1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1-249	ETP-C-000249-CAG2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1-249	ETP-C-000249-CAG3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1-249	ETP-C-000249-CAG4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1-249	ETP-C-000249-CAG5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1-249	ETP-C-000249-CAP1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1-249	ETP-C-000249-CAP2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1-249	ETP-C-000249-CAP3Y	$ 237.98	$ 207.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1-249	ETP-C-000249-CAP4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1-249	ETP-C-000249-CAP5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1-249	ETP-C-000249-PPL1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1-249	ETP-C-000249-PPL2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1-249	ETP-C-000249-PPL3Y	$ 237.98	$ 207.04
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1-249	ETP-C-000249-PPL4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1-249	ETP-C-000249-PPL5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1-249	ETP-C-000249-PTM1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1-249	ETP-C-000249-PTM2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1-249	ETP-C-000249-PTM3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1-249	ETP-C-000249-PTM4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1-249	ETP-C-000249-PTM5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1-249	ETP-C-000249-USG1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1-249	ETP-C-000249-USG2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1-249	ETP-C-000249-USG3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1-249	ETP-C-000249-USG4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1-249	ETP-C-000249-USG5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1-249	ETP-C-000249-USP1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1-249	ETP-C-000249-USP2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1-249	ETP-C-000249-USP3Y	$ 237.98	$ 207.04

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1-249	ETP-C-000249-USP4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1-249	ETP-C-000249-USP5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 250-499	ETP-C-000499-CAG1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 250-499	ETP-C-000499-CAG2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 250-499	ETP-C-000499-CAG3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 250-499	ETP-C-000499-CAG4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 250-499	ETP-C-000499-CAG5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 250-499	ETP-C-000499-CAP1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 250-499	ETP-C-000499-CAP2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 250-499	ETP-C-000499-CAP3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 250-499	ETP-C-000499-CAP4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 250-499	ETP-C-000499-CAP5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 250-499	ETP-C-000499-PPL1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 250-499	ETP-C-000499-PPL2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 250-499	ETP-C-000499-PPL3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 250-499	ETP-C-000499-PPL4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 250-499	ETP-C-000499-PPL5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 250-499	ETP-C-000499-PTM1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 250-499	ETP-C-000499-PTM2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 250-499	ETP-C-000499-PTM3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 250-499	ETP-C-000499-PTM4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 250-499	ETP-C-000499-PTM5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 250-499	ETP-C-000499-USG1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 250-499	ETP-C-000499-USG2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 250-499	ETP-C-000499-USG3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 250-499	ETP-C-000499-USG4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 250-499	ETP-C-000499-USG5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 250-499	ETP-C-000499-USP1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 250-499	ETP-C-000499-USP2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 250-499	ETP-C-000499-USP3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 250-499	ETP-C-000499-USP4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 250-499	ETP-C-000499-USP5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 500-749	ETP-C-000749-CAG1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 500-749	ETP-C-000749-CAG2Y	$ 119.78	$ 104.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 500-749	ETP-C-000749-CAG3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 500-749	ETP-C-000749-CAG4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 500-749	ETP-C-000749-CAG5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 500-749	ETP-C-000749-CAP1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 500-749	ETP-C-000749-CAP2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 500-749	ETP-C-000749-CAP3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 500-749	ETP-C-000749-CAP4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 500-749	ETP-C-000749-CAP5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 500-749	ETP-C-000749-PPL1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 500-749	ETP-C-000749-PPL2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 500-749	ETP-C-000749-PPL3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 500-749	ETP-C-000749-PPL4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 500-749	ETP-C-000749-PPL5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 500-749	ETP-C-000749-PTM1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 500-749	ETP-C-000749-PTM2Y	$ 119.78	$ 104.21

FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 500-749	ETP-C-000749-PTM3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 500-749	ETP-C-000749-PTM4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 500-749	ETP-C-000749-PTM5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 500-749	ETP-C-000749-USG1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 500-749	ETP-C-000749-USG2Y	$ 119.78	$ 104.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 500-749	ETP-C-000749-USG3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 500-749	ETP-C-000749-USG4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 500-749	ETP-C-000749-USG5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 500-749	ETP-C-000749-USP1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 500-749	ETP-C-000749-USP2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 500-749	ETP-C-000749-USP3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 500-749	ETP-C-000749-USP4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 500-749	ETP-C-000749-USP5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 750-999	ETP-C-000999-CAG1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 750-999	ETP-C-000999-CAG2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 750-999	ETP-C-000999-CAG3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 750-999	ETP-C-000999-CAG4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 750-999	ETP-C-000999-CAG5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 750-999	ETP-C-000999-CAP1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 750-999	ETP-C-000999-CAP2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 750-999	ETP-C-000999-CAP3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 750-999	ETP-C-000999-CAP4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 750-999	ETP-C-000999-CAP5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 750-999	ETP-C-000999-PPL1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 750-999	ETP-C-000999-PPL2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 750-999	ETP-C-000999-PPL3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 750-999	ETP-C-000999-PPL4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 750-999	ETP-C-000999-PPL5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 750-999	ETP-C-000999-PTM1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 750-999	ETP-C-000999-PTM2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 750-999	ETP-C-000999-PTM3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 750-999	ETP-C-000999-PTM4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 750-999	ETP-C-000999-PTM5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 750-999	ETP-C-000999-USG1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 750-999	ETP-C-000999-USG2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 750-999	ETP-C-000999-USG3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 750-999	ETP-C-000999-USG4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 750-999	ETP-C-000999-USG5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 750-999	ETP-C-000999-USP1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 750-999	ETP-C-000999-USP2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 750-999	ETP-C-000999-USP3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 750-999	ETP-C-000999-USP4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 750-999	ETP-C-000999-USP5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1,000-1999	ETP-C-001999-CAG1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1,000-1999	ETP-C-001999-CAG2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1,000-1999	ETP-C-001999-CAG3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1,000-1999	ETP-C-001999-CAG4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1,000-1999	ETP-C-001999-CAG5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1,000-1999	ETP-C-001999-CAP1Y	$ 47.55	$ 41.37

FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1,000-1999	ETP-C-001999-CAP2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1,000-1999	ETP-C-001999-CAP3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1,000-1999	ETP-C-001999-CAP4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1,000-1999	ETP-C-001999-CAP5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1,000-1999	ETP-C-001999-PPL1Y	$ 47.55	$ 41.37
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1,000-1999	ETP-C-001999-PPL2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1,000-1999	ETP-C-001999-PPL3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1,000-1999	ETP-C-001999-PPL4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1,000-1999	ETP-C-001999-PPL5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1,000-1999	ETP-C-001999-PTM1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1,000-1999	ETP-C-001999-PTM2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1,000-1999	ETP-C-001999-PTM3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1,000-1999	ETP-C-001999-PTM4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1,000-1999	ETP-C-001999-PTM5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1,000-1999	ETP-C-001999-USG1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1,000-1999	ETP-C-001999-USG2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1,000-1999	ETP-C-001999-USG3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1,000-1999	ETP-C-001999-USG4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1,000-1999	ETP-C-001999-USG5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-C-001999-USP1Y	$ 47.55	$ 41.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-C-001999-USP2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-C-001999-USP3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-C-001999-USP4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-C-001999-USP5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 2,000-4999	ETP-C-004999-CAG1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 2,000-4999	ETP-C-004999-CAG2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 2,000-4999	ETP-C-004999-CAG3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 2,000-4999	ETP-C-004999-CAG4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 2,000-4999	ETP-C-004999-CAG5Y	$ 186.89	$ 162.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 2,000-4999	ETP-C-004999-CAP1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 2,000-4999	ETP-C-004999-CAP2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 2,000-4999	ETP-C-004999-CAP3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 2,000-4999	ETP-C-004999-CAP4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 2,000-4999	ETP-C-004999-CAP5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 2,000-4999	ETP-C-004999-PPL1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 2,000-4999	ETP-C-004999-PPL2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 2,000-4999	ETP-C-004999-PPL3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 2,000-4999	ETP-C-004999-PPL4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 2,000-4999	ETP-C-004999-PPL5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 2,000-4999	ETP-C-004999-PTM1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 2,000-4999	ETP-C-004999-PTM2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 2,000-4999	ETP-C-004999-PTM3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 2,000-4999	ETP-C-004999-PTM4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 2,000-4999	ETP-C-004999-PTM5Y	$ 186.89	$ 162.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 2,000-4999	ETP-C-004999-USG1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 2,000-4999	ETP-C-004999-USG2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 2,000-4999	ETP-C-004999-USG3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 2,000-4999	ETP-C-004999-USG4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 2,000-4999	ETP-C-004999-USG5Y	$ 186.89	$ 162.59

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-C-004999-USP1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-C-004999-USP2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-C-004999-USP3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-C-004999-USP4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-C-004999-USP5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 5,000-9999	ETP-C-009999-CAG1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 5,000-9999	ETP-C-009999-CAG2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 5,000-9999	ETP-C-009999-CAG3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 5,000-9999	ETP-C-009999-CAG4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 5,000-9999	ETP-C-009999-CAG5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 5,000-9999	ETP-C-009999-CAP1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 5,000-9999	ETP-C-009999-CAP2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 5,000-9999	ETP-C-009999-CAP3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 5,000-9999	ETP-C-009999-CAP4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 5,000-9999	ETP-C-009999-CAP5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 5,000-9999	ETP-C-009999-PPL1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 5,000-9999	ETP-C-009999-PPL2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 5,000-9999	ETP-C-009999-PPL3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 5,000-9999	ETP-C-009999-PPL4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 5,000-9999	ETP-C-009999-PPL5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 5,000-9999	ETP-C-009999-PTM1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 5,000-9999	ETP-C-009999-PTM2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 5,000-9999	ETP-C-009999-PTM3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 5,000-9999	ETP-C-009999-PTM4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 5,000-9999	ETP-C-009999-PTM5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 5,000-9999	ETP-C-009999-USG1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 5,000-9999	ETP-C-009999-USG2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 5,000-9999	ETP-C-009999-USG3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 5,000-9999	ETP-C-009999-USG4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 5,000-9999	ETP-C-009999-USG5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-C-009999-USP1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-C-009999-USP2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-C-009999-USP3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-C-009999-USP4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-C-009999-USP5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 10,000-19999	ETP-C-019999-CAG1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 10,000-19999	ETP-C-019999-CAG2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 10,000-19999	ETP-C-019999-CAG3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 10,000-19999	ETP-C-019999-CAG4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 10,000-19999	ETP-C-019999-CAG5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 10,000-19999	ETP-C-019999-CAP1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 10,000-19999	ETP-C-019999-CAP2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 10,000-19999	ETP-C-019999-CAP3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 10,000-19999	ETP-C-019999-CAP4Y	$ 123.12	$ 107.11
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 10,000-19999	ETP-C-019999-CAP5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 10,000-19999	ETP-C-019999-PPL1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 10,000-19999	ETP-C-019999-PPL2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 10,000-19999	ETP-C-019999-PPL3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 10,000-19999	ETP-C-019999-PPL4Y	$ 123.12	$ 107.11

FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 10,000-19999	ETP-C-019999-PPL5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 10,000-19999	ETP-C-019999-PTM1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 10,000-19999	ETP-C-019999-PTM2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 10,000-19999	ETP-C-019999-PTM3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 10,000-19999	ETP-C-019999-PTM4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 10,000-19999	ETP-C-019999-PTM5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 10,000-19999	ETP-C-019999-USG1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 10,000-19999	ETP-C-019999-USG2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 10,000-19999	ETP-C-019999-USG3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 10,000-19999	ETP-C-019999-USG4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 10,000-19999	ETP-C-019999-USG5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-C-019999-USP1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-C-019999-USP2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-C-019999-USP3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-C-019999-USP4Y	$ 123.12	$ 107.11
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-C-019999-USP5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 20,000-49999	ETP-C-049999-CAG1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 20,000-49999	ETP-C-049999-CAG2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 20,000-49999	ETP-C-049999-CAG3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 20,000-49999	ETP-C-049999-CAG4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 20,000-49999	ETP-C-049999-CAG5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 20,000-49999	ETP-C-049999-CAP1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 20,000-49999	ETP-C-049999-CAP2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 20,000-49999	ETP-C-049999-CAP3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 20,000-49999	ETP-C-049999-CAP4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 20,000-49999	ETP-C-049999-CAP5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 20,000-49999	ETP-C-049999-PPL1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 20,000-49999	ETP-C-049999-PPL2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 20,000-49999	ETP-C-049999-PPL3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 20,000-49999	ETP-C-049999-PPL4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 20,000-49999	ETP-C-049999-PPL5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 20,000-49999	ETP-C-049999-PTM1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 20,000-49999	ETP-C-049999-PTM2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 20,000-49999	ETP-C-049999-PTM3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 20,000-49999	ETP-C-049999-PTM4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 20,000-49999	ETP-C-049999-PTM5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 20,000-49999	ETP-C-049999-USG1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 20,000-49999	ETP-C-049999-USG2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 20,000-49999	ETP-C-049999-USG3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 20,000-49999	ETP-C-049999-USG4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 20,000-49999	ETP-C-049999-USG5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-C-049999-USP1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-C-049999-USP2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-C-049999-USP3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-C-049999-USP4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-C-049999-USP5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 50,000-74999	ETP-C-074999-CAG1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 50,000-74999	ETP-C-074999-CAG2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 50,000-74999	ETP-C-074999-CAG3Y	$ 74.39	$ 64.72

FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 50,000-74999	ETP-C-074999-CAG4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 50,000-74999	ETP-C-074999-CAG5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 50,000-74999	ETP-C-074999-CAP1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 50,000-74999	ETP-C-074999-CAP2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 50,000-74999	ETP-C-074999-CAP3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 50,000-74999	ETP-C-074999-CAP4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 50,000-74999	ETP-C-074999-CAP5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 50,000-74999	ETP-C-074999-PPL1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 50,000-74999	ETP-C-074999-PPL2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 50,000-74999	ETP-C-074999-PPL3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 50,000-74999	ETP-C-074999-PPL4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 50,000-74999	ETP-C-074999-PPL5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 50,000-74999	ETP-C-074999-PTM1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 50,000-74999	ETP-C-074999-PTM2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 50,000-74999	ETP-C-074999-PTM3Y	$ 74.39	$ 64.72
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 50,000-74999	ETP-C-074999-PTM4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 50,000-74999	ETP-C-074999-PTM5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 50,000-74999	ETP-C-074999-USG1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 50,000-74999	ETP-C-074999-USG2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 50,000-74999	ETP-C-074999-USG3Y	$ 74.39	$ 64.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 50,000-74999	ETP-C-074999-USG4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 50,000-74999	ETP-C-074999-USG5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-C-074999-USP1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-C-074999-USP2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-C-074999-USP3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-C-074999-USP4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-C-074999-USP5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 75,000-99999	ETP-C-099999-CAG1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 75,000-99999	ETP-C-099999-CAG2Y	$ 48.88	$ 42.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 75,000-99999	ETP-C-099999-CAG3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 75,000-99999	ETP-C-099999-CAG4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 75,000-99999	ETP-C-099999-CAG5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 75,000-99999	ETP-C-099999-CAP1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 75,000-99999	ETP-C-099999-CAP2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 75,000-99999	ETP-C-099999-CAP3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 75,000-99999	ETP-C-099999-CAP4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 75,000-99999	ETP-C-099999-CAP5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 75,000-99999	ETP-C-099999-PPL1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 75,000-99999	ETP-C-099999-PPL2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 75,000-99999	ETP-C-099999-PPL3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 75,000-99999	ETP-C-099999-PPL4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 75,000-99999	ETP-C-099999-PPL5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 75,000-99999	ETP-C-099999-PTM1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 75,000-99999	ETP-C-099999-PTM2Y	$ 48.88	$ 42.53
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 75,000-99999	ETP-C-099999-PTM3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 75,000-99999	ETP-C-099999-PTM4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 75,000-99999	ETP-C-099999-PTM5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 75,000-99999	ETP-C-099999-USG1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 75,000-99999	ETP-C-099999-USG2Y	$ 48.88	$ 42.53

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 75,000-99999	ETP-C-099999-USG3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 75,000-99999	ETP-C-099999-USG4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 75,000-99999	ETP-C-099999-USG5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-C-099999-USP1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-C-099999-USP2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-C-099999-USP3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-C-099999-USP4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-C-099999-USP5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 100,000-199999	ETP-C-199999-CAG1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 100,000-199999	ETP-C-199999-CAG2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 100,000-199999	ETP-C-199999-CAG3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 100,000-199999	ETP-C-199999-CAG4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 100,000-199999	ETP-C-199999-CAG5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 100,000-199999	ETP-C-199999-CAP1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 100,000-199999	ETP-C-199999-CAP2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 100,000-199999	ETP-C-199999-CAP3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 100,000-199999	ETP-C-199999-CAP4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 100,000-199999	ETP-C-199999-CAP5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 100,000-199999	ETP-C-199999-PPL1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 100,000-199999	ETP-C-199999-PPL2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 100,000-199999	ETP-C-199999-PPL3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 100,000-199999	ETP-C-199999-PPL4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 100,000-199999	ETP-C-199999-PPL5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 100,000-199999	ETP-C-199999-PTM1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 100,000-199999	ETP-C-199999-PTM2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 100,000-199999	ETP-C-199999-PTM3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 100,000-199999	ETP-C-199999-PTM4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 100,000-199999	ETP-C-199999-PTM5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 100,000-199999	ETP-C-199999-USG1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 100,000-199999	ETP-C-199999-USG2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 100,000-199999	ETP-C-199999-USG3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 100,000-199999	ETP-C-199999-USG4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 100,000-199999	ETP-C-199999-USG5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-C-199999-USP1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-C-199999-USP2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-C-199999-USP3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-C-199999-USP4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-C-199999-USP5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 200,000+	ETP-C-200000+CAG1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 200,000+	ETP-C-200000+CAG2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 200,000+	ETP-C-200000+CAG3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 200,000+	ETP-C-200000+CAG4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 200,000+	ETP-C-200000+CAG5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 200,000+	ETP-C-200000+CAP1Y	$ 20.33	$ 17.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 200,000+	ETP-C-200000+CAP2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 200,000+	ETP-C-200000+CAP3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 200,000+	ETP-C-200000+CAP4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 200,000+	ETP-C-200000+CAP5Y	$ 91.49	$ 79.60
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 200,000+	ETP-C-200000+PPL1Y	$ 20.33	$ 17.69

FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 200,000+	ETP-C-200000+PPL2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 200,000+	ETP-C-200000+PPL3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 200,000+	ETP-C-200000+PPL4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 200,000+	ETP-C-200000+PPL5Y	$ 91.49	$ 79.60
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 200,000+	ETP-C-200000+PTM1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 200,000+	ETP-C-200000+PTM2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 200,000+	ETP-C-200000+PTM3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 200,000+	ETP-C-200000+PTM4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 200,000+	ETP-C-200000+PTM5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 200,000+	ETP-C-200000+USG1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 200,000+	ETP-C-200000+USG2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 200,000+	ETP-C-200000+USG3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 200,000+	ETP-C-200000+USG4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 200,000+	ETP-C-200000+USG5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 200,000+	ETP-C-200000+USP1Y	$ 20.33	$ 17.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 200,000+	ETP-C-200000+USP2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 200,000+	ETP-C-200000+USP3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 200,000+	ETP-C-200000+USP4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 200,000+	ETP-C-200000+USP5Y	$ 91.49	$ 79.60
FireEye	EVL Email Threat Prevention	EVL-EC-ETP	$ -	$ -
FireEye	EVL AV/AS Add-on for ETP Cloud with AV/AS	EVL-EC-ETP-A	$ -	$ -
FireEye	EVL Email Threat Prevention Cloud with AV/AS	EVL-EC-ETP-C	$ -	$ -
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 1-249	RN-ETP-000249-PTM1Y	$ 58.32	$ 50.74
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 1-249	RN-ETP-000249-PTM3Y	$ 157.46	$ 136.99
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 1-249	RN-ETP-000249-PTM4Y	$ 209.95	$ 182.66
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 1-249	RN-ETP-000249-PTM5Y	$ 262.44	$ 228.32
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 1-249	RN-ETP-000249-USG1Y	$ 58.32	$ 50.74
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 1-249	RN-ETP-000249-USG3Y	$ 157.46	$ 136.99
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 1-249	RN-ETP-000249-USG4Y	$ 209.95	$ 182.66
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 1-249	RN-ETP-000249-USG5Y	$ 262.44	$ 228.32
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 250-499	RN-ETP-000499-PTM1Y	$ 48.15	$ 41.89
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 250-499	RN-ETP-000499-PTM3Y	$ 130.01	$ 113.11
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 250-499	RN-ETP-000499-PTM4Y	$ 173.34	$ 150.81
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 250-499	RN-ETP-000499-PTM5Y	$ 216.68	$ 188.51
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 250-499	RN-ETP-000499-USG1Y	$ 48.15	$ 41.89
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 250-499	RN-ETP-000499-USG3Y	$ 130.01	$ 113.11
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 250-499	RN-ETP-000499-USG4Y	$ 173.34	$ 150.81
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 250-499	RN-ETP-000499-USG5Y	$ 216.68	$ 188.51
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 500-749	RN-ETP-000749-PTM1Y	$ 41.30	$ 35.93
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 500-749	RN-ETP-000749-PTM3Y	$ 111.51	$ 97.01
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 500-749	RN-ETP-000749-PTM4Y	$ 148.68	$ 129.35
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 500-749	RN-ETP-000749-PTM5Y	$ 185.85	$ 161.69
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 500-749	RN-ETP-000749-USG1Y	$ 41.30	$ 35.93
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 500-749	RN-ETP-000749-USG3Y	$ 111.51	$ 97.01
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 500-749	RN-ETP-000749-USG4Y	$ 148.68	$ 129.35
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 500-749	RN-ETP-000749-USG5Y	$ 185.85	$ 161.69
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 750-999	RN-ETP-000999-PTM1Y	$ 34.69	$ 30.18
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 750-999	RN-ETP-000999-PTM3Y	$ 93.66	$ 81.48
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 750-999	RN-ETP-000999-PTM4Y	$ 124.88	$ 108.65

FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 750-999	RN-ETP-000999-PTM5Y	$ 156.11	$ 135.82
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 750-999	RN-ETP-000999-USG1Y	$ 34.69	$ 30.18
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 750-999	RN-ETP-000999-USG3Y	$ 93.66	$ 81.48
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 750-999	RN-ETP-000999-USG4Y	$ 124.88	$ 108.65
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 750-999	RN-ETP-000999-USG5Y	$ 156.11	$ 135.82
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 1,000-1999	RN-ETP-001999-PTM1Y	$ 31.46	$ 27.37
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 1,000-1999	RN-ETP-001999-PTM3Y	$ 84.94	$ 73.90
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 1,000-1999	RN-ETP-001999-PTM4Y	$ 113.26	$ 98.54
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 1,000-1999	RN-ETP-001999-PTM5Y	$ 141.57	$ 123.17
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 1,000-1999	RN-ETP-001999-USG1Y	$ 31.46	$ 27.37
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 1,000-1999	RN-ETP-001999-USG3Y	$ 84.94	$ 73.90
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 1,000-1999	RN-ETP-001999-USG4Y	$ 113.26	$ 98.54
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 1,000-1999	RN-ETP-001999-USG5Y	$ 141.57	$ 123.17
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 2,000-4999	RN-ETP-004999-PTM1Y	$ 28.64	$ 24.92
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 2,000-4999	RN-ETP-004999-PTM3Y	$ 77.33	$ 67.28
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 2,000-4999	RN-ETP-004999-PTM4Y	$ 103.10	$ 89.70
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 2,000-4999	RN-ETP-004999-PTM5Y	$ 128.88	$ 112.13
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 2,000-4999	RN-ETP-004999-USG1Y	$ 28.64	$ 24.92
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 2,000-4999	RN-ETP-004999-USG3Y	$ 77.33	$ 67.28
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 2,000-4999	RN-ETP-004999-USG4Y	$ 103.10	$ 89.70
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 2,000-4999	RN-ETP-004999-USG5Y	$ 128.88	$ 112.13
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 5,000-9999	RN-ETP-009999-PTM1Y	$ 25.51	$ 22.19
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 5,000-9999	RN-ETP-009999-PTM3Y	$ 68.88	$ 59.93
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 5,000-9999	RN-ETP-009999-PTM4Y	$ 91.84	$ 79.90
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 5,000-9999	RN-ETP-009999-PTM5Y	$ 114.80	$ 99.88
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 5,000-9999	RN-ETP-009999-USG1Y	$ 25.51	$ 22.19
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 5,000-9999	RN-ETP-009999-USG3Y	$ 68.88	$ 59.93
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 5,000-9999	RN-ETP-009999-USG4Y	$ 91.84	$ 79.90
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 5,000-9999	RN-ETP-009999-USG5Y	$ 114.80	$ 99.88
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 10,000-19999	RN-ETP-019999-PTM1Y	$ 22.02	$ 19.16
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 10,000-19999	RN-ETP-019999-PTM3Y	$ 59.45	$ 51.72
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 10,000-19999	RN-ETP-019999-PTM4Y	$ 79.27	$ 68.96
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 10,000-19999	RN-ETP-019999-PTM5Y	$ 99.09	$ 86.21
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 10,000-19999	RN-ETP-019999-USG1Y	$ 22.02	$ 19.16
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 10,000-19999	RN-ETP-019999-USG3Y	$ 59.45	$ 51.72
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 10,000-19999	RN-ETP-019999-USG4Y	$ 79.27	$ 68.96
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 10,000-19999	RN-ETP-019999-USG5Y	$ 99.09	$ 86.21
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 20,000-49999	RN-ETP-049999-PTM1Y	$ 20.76	$ 18.06
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 20,000-49999	RN-ETP-049999-PTM3Y	$ 56.05	$ 48.76
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 20,000-49999	RN-ETP-049999-PTM4Y	$ 74.74	$ 65.02
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 20,000-49999	RN-ETP-049999-PTM5Y	$ 93.42	$ 81.28
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 20,000-49999	RN-ETP-049999-USG1Y	$ 20.76	$ 18.06
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 20,000-49999	RN-ETP-049999-USG3Y	$ 56.05	$ 48.76
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 20,000-49999	RN-ETP-049999-USG4Y	$ 74.74	$ 65.02
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 20,000-49999	RN-ETP-049999-USG5Y	$ 93.42	$ 81.28
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 50,000-74999	RN-ETP-074999-PTM1Y	$ 18.75	$ 16.31
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 50,000-74999	RN-ETP-074999-PTM3Y	$ 50.63	$ 44.05
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 50,000-74999	RN-ETP-074999-PTM4Y	$ 67.50	$ 58.73
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 50,000-74999	RN-ETP-074999-PTM5Y	$ 84.38	$ 73.41

FireEye	Renewal-Email Threat Prevention, Government US 1 Year 50,000-74999	RN-ETP-074999-USG1Y	$ 18.75	$ 16.31
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 50,000-74999	RN-ETP-074999-USG3Y	$ 50.63	$ 44.05
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 50,000-74999	RN-ETP-074999-USG4Y	$ 67.50	$ 58.73
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 50,000-74999	RN-ETP-074999-USG5Y	$ 84.38	$ 73.41
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 75,000-99999	RN-ETP-099999-PTM1Y	$ 16.22	$ 14.11
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 75,000-99999	RN-ETP-099999-PTM3Y	$ 43.79	$ 38.10
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 75,000-99999	RN-ETP-099999-PTM4Y	$ 58.39	$ 50.80
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 75,000-99999	RN-ETP-099999-PTM5Y	$ 72.99	$ 63.50
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 75,000-99999	RN-ETP-099999-USG1Y	$ 16.22	$ 14.11
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 75,000-99999	RN-ETP-099999-USG3Y	$ 43.79	$ 38.10
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 75,000-99999	RN-ETP-099999-USG4Y	$ 58.39	$ 50.80
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 75,000-99999	RN-ETP-099999-USG5Y	$ 72.99	$ 63.50
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 100,000-199999	RN-ETP-199999-PTM1Y	$ 14.26	$ 12.41
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 100,000-199999	RN-ETP-199999-PTM3Y	$ 38.50	$ 33.50
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 100,000-199999	RN-ETP-199999-PTM4Y	$ 51.34	$ 44.67
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 100,000-199999	RN-ETP-199999-PTM5Y	$ 64.17	$ 55.83
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 100,000-199999	RN-ETP-199999-USG1Y	$ 14.26	$ 12.41
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 100,000-199999	RN-ETP-199999-USG3Y	$ 38.50	$ 33.50
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 100,000-199999	RN-ETP-199999-USG4Y	$ 51.34	$ 44.67
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 100,000-199999	RN-ETP-199999-USG5Y	$ 64.17	$ 55.83
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 200,000+	RN-ETP-200000+PTM1Y	$ 13.46	$ 11.71
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 200,000+	RN-ETP-200000+PTM3Y	$ 36.34	$ 31.62
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 200,000+	RN-ETP-200000+PTM4Y	$ 48.46	$ 42.16
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 200,000+	RN-ETP-200000+PTM5Y	$ 60.57	$ 52.70
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 200,000+	RN-ETP-200000+USG1Y	$ 13.46	$ 11.71
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 200,000+	RN-ETP-200000+USG3Y	$ 36.34	$ 31.62
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 200,000+	RN-ETP-200000+USG4Y	$ 48.46	$ 42.16
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 200,000+	RN-ETP-200000+USG5Y	$ 60.57	$ 52.70
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1-249	RN-ETP-A-000249-CAG1Y	$ 71.95	$ 62.60
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1-249	RN-ETP-A-000249-CAG2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1-249	RN-ETP-A-000249-CAG3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1-249	RN-ETP-A-000249-CAG4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1-249	RN-ETP-A-000249-CAG5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1-249	RN-ETP-A-000249-CAP1Y	$ 75.00	$ 65.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1-249	RN-ETP-A-000249-CAP2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1-249	RN-ETP-A-000249-CAP3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1-249	RN-ETP-A-000249-CAP4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1-249	RN-ETP-A-000249-CAP5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1-249	RN-ETP-A-000249-PPL1Y	$ 13.62	$ 11.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1-249	RN-ETP-A-000249-PPL2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1-249	RN-ETP-A-000249-PPL3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1-249	RN-ETP-A-000249-PPL4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1-249	RN-ETP-A-000249-PPL5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1-249	RN-ETP-A-000249-PTM1Y	$ 26.24	$ 22.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1-249	RN-ETP-A-000249-PTM2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1-249	RN-ETP-A-000249-PTM3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1-249	RN-ETP-A-000249-PTM4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1-249	RN-ETP-A-000249-PTM5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 1-249	RN-ETP-A-000249-USG1Y	$ 71.95	$ 62.60

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 1-249	RN-ETP-A-000249-USG2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 1-249	RN-ETP-A-000249-USG3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 1-249	RN-ETP-A-000249-USG4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 1-249	RN-ETP-A-000249-USG5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-A-000249-USP1Y	$ 75.00	$ 65.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-A-000249-USP2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-A-000249-USP3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-A-000249-USP4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1-249	RN-ETP-A-000249-USP5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 250-499	RN-ETP-A-000499-CAG1Y	$ 35.96	$ 31.29
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 250-499	RN-ETP-A-000499-CAG2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 250-499	RN-ETP-A-000499-CAG3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 250-499	RN-ETP-A-000499-CAG4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 250-499	RN-ETP-A-000499-CAG5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 250-499	RN-ETP-A-000499-CAP1Y	$ 37.48	$ 32.61
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 250-499	RN-ETP-A-000499-CAP2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 250-499	RN-ETP-A-000499-CAP3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 250-499	RN-ETP-A-000499-CAP4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 250-499	RN-ETP-A-000499-CAP5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 250-499	RN-ETP-A-000499-PPL1Y	$ 11.26	$ 9.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 250-499	RN-ETP-A-000499-PPL2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 250-499	RN-ETP-A-000499-PPL3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 250-499	RN-ETP-A-000499-PPL4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 250-499	RN-ETP-A-000499-PPL5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 250-499	RN-ETP-A-000499-PTM1Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 250-499	RN-ETP-A-000499-PTM2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 250-499	RN-ETP-A-000499-PTM3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 250-499	RN-ETP-A-000499-PTM4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 250-499	RN-ETP-A-000499-PTM5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 250-499	RN-ETP-A-000499-USG1Y	$ 35.96	$ 31.29
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 250-499	RN-ETP-A-000499-USG2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 250-499	RN-ETP-A-000499-USG3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 250-499	RN-ETP-A-000499-USG4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 250-499	RN-ETP-A-000499-USG5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-A-000499-USP1Y	$ 37.48	$ 32.61
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-A-000499-USP2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-A-000499-USP3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-A-000499-USP4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 250-499	RN-ETP-A-000499-USP5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 500-749	RN-ETP-A-000749-CAG1Y	$ 29.76	$ 25.89
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 500-749	RN-ETP-A-000749-CAG2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 500-749	RN-ETP-A-000749-CAG3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 500-749	RN-ETP-A-000749-CAG4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 500-749	RN-ETP-A-000749-CAG5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 500-749	RN-ETP-A-000749-CAP1Y	$ 31.02	$ 26.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 500-749	RN-ETP-A-000749-CAP2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 500-749	RN-ETP-A-000749-CAP3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 500-749	RN-ETP-A-000749-CAP4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 500-749	RN-ETP-A-000749-CAP5Y	$ 139.59	$ 121.44

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 500-749	RN-ETP-A-000749-PPL1Y	$ 9.66	$ 8.40
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 500-749	RN-ETP-A-000749-PPL2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 500-749	RN-ETP-A-000749-PPL3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 500-749	RN-ETP-A-000749-PPL4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 500-749	RN-ETP-A-000749-PPL5Y	$ 139.59	$ 121.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 500-749	RN-ETP-A-000749-PTM1Y	$ 18.59	$ 16.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 500-749	RN-ETP-A-000749-PTM2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 500-749	RN-ETP-A-000749-PTM3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 500-749	RN-ETP-A-000749-PTM4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 500-749	RN-ETP-A-000749-PTM5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 500-749	RN-ETP-A-000749-USG1Y	$ 29.76	$ 25.89
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 500-749	RN-ETP-A-000749-USG2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 500-749	RN-ETP-A-000749-USG3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 500-749	RN-ETP-A-000749-USG4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 500-749	RN-ETP-A-000749-USG5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-A-000749-USP1Y	$ 31.02	$ 26.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-A-000749-USP2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-A-000749-USP3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-A-000749-USP4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 500-749	RN-ETP-A-000749-USP5Y	$ 139.59	$ 121.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 750-999	RN-ETP-A-000999-CAG1Y	$ 29.03	$ 25.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 750-999	RN-ETP-A-000999-CAG2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 750-999	RN-ETP-A-000999-CAG3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 750-999	RN-ETP-A-000999-CAG4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 750-999	RN-ETP-A-000999-CAG5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 750-999	RN-ETP-A-000999-CAP1Y	$ 30.26	$ 26.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 750-999	RN-ETP-A-000999-CAP2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 750-999	RN-ETP-A-000999-CAP3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 750-999	RN-ETP-A-000999-CAP4Y	$ 108.94	$ 94.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 750-999	RN-ETP-A-000999-CAP5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 750-999	RN-ETP-A-000999-PPL1Y	$ 8.11	$ 7.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 750-999	RN-ETP-A-000999-PPL2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 750-999	RN-ETP-A-000999-PPL3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 750-999	RN-ETP-A-000999-PPL4Y	$ 108.94	$ 94.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 750-999	RN-ETP-A-000999-PPL5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 750-999	RN-ETP-A-000999-PTM1Y	$ 15.61	$ 13.58
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 750-999	RN-ETP-A-000999-PTM2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 750-999	RN-ETP-A-000999-PTM3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 750-999	RN-ETP-A-000999-PTM4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 750-999	RN-ETP-A-000999-PTM5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 750-999	RN-ETP-A-000999-USG1Y	$ 29.03	$ 25.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 750-999	RN-ETP-A-000999-USG2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 750-999	RN-ETP-A-000999-USG3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 750-999	RN-ETP-A-000999-USG4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 750-999	RN-ETP-A-000999-USG5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-A-000999-USP1Y	$ 30.26	$ 26.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-A-000999-USP2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-A-000999-USP3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-A-000999-USP4Y	$ 108.94	$ 94.78

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 750-999	RN-ETP-A-000999-USP5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1,000-1999	RN-ETP-A-001999-CAG1Y	$ 22.35	$ 19.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1,000-1999	RN-ETP-A-001999-CAG2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1,000-1999	RN-ETP-A-001999-CAG3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1,000-1999	RN-ETP-A-001999-CAG4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1,000-1999	RN-ETP-A-001999-CAG5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1,000-1999	RN-ETP-A-001999-CAP1Y	$ 23.29	$ 20.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1,000-1999	RN-ETP-A-001999-CAP2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1,000-1999	RN-ETP-A-001999-CAP3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1,000-1999	RN-ETP-A-001999-CAP4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1,000-1999	RN-ETP-A-001999-CAP5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-A-001999-PPL1Y	$ 7.35	$ 6.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-A-001999-PPL2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-A-001999-PPL3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-A-001999-PPL4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1,000-1999	RN-ETP-A-001999-PPL5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1,000-1999	RN-ETP-A-001999-PTM1Y	$ 14.16	$ 12.32
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1,000-1999	RN-ETP-A-001999-PTM2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1,000-1999	RN-ETP-A-001999-PTM3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1,000-1999	RN-ETP-A-001999-PTM4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1,000-1999	RN-ETP-A-001999-PTM5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 1,000-1999	RN-ETP-A-001999-USG1Y	$ 22.35	$ 19.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 1,000-1999	RN-ETP-A-001999-USG2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 1,000-1999	RN-ETP-A-001999-USG3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 1,000-1999	RN-ETP-A-001999-USG4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 1,000-1999	RN-ETP-A-001999-USG5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-A-001999-USP1Y	$ 23.29	$ 20.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-A-001999-USP2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-A-001999-USP3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-A-001999-USP4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1,000-1999	RN-ETP-A-001999-USP5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 2,000-4999	RN-ETP-A-004999-CAG1Y	$ 16.67	$ 14.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 2,000-4999	RN-ETP-A-004999-CAG2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 2,000-4999	RN-ETP-A-004999-CAG3Y	$ 45.01	$ 39.16
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 2,000-4999	RN-ETP-A-004999-CAG4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 2,000-4999	RN-ETP-A-004999-CAG5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 2,000-4999	RN-ETP-A-004999-CAP1Y	$ 17.38	$ 15.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 2,000-4999	RN-ETP-A-004999-CAP2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 2,000-4999	RN-ETP-A-004999-CAP3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 2,000-4999	RN-ETP-A-004999-CAP4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 2,000-4999	RN-ETP-A-004999-CAP5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-A-004999-PPL1Y	$ 6.70	$ 5.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-A-004999-PPL2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-A-004999-PPL3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-A-004999-PPL4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 2,000-4999	RN-ETP-A-004999-PPL5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 2,000-4999	RN-ETP-A-004999-PTM1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 2,000-4999	RN-ETP-A-004999-PTM2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 2,000-4999	RN-ETP-A-004999-PTM3Y	$ 45.01	$ 39.16

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 2,000-4999	RN-ETP-A-004999-PTM4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 2,000-4999	RN-ETP-A-004999-PTM5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 2,000-4999	RN-ETP-A-004999-USG1Y	$ 16.67	$ 14.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 2,000-4999	RN-ETP-A-004999-USG2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 2,000-4999	RN-ETP-A-004999-USG3Y	$ 45.01	$ 39.16
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 2,000-4999	RN-ETP-A-004999-USG4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 2,000-4999	RN-ETP-A-004999-USG5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-A-004999-USP1Y	$ 17.38	$ 15.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-A-004999-USP2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-A-004999-USP3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-A-004999-USP4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 2,000-4999	RN-ETP-A-004999-USP5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 5,000-9999	RN-ETP-A-009999-CAG1Y	$ 14.75	$ 12.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 5,000-9999	RN-ETP-A-009999-CAG2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 5,000-9999	RN-ETP-A-009999-CAG3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 5,000-9999	RN-ETP-A-009999-CAG4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 5,000-9999	RN-ETP-A-009999-CAG5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 5,000-9999	RN-ETP-A-009999-CAP1Y	$ 15.37	$ 13.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 5,000-9999	RN-ETP-A-009999-CAP2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 5,000-9999	RN-ETP-A-009999-CAP3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 5,000-9999	RN-ETP-A-009999-CAP4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 5,000-9999	RN-ETP-A-009999-CAP5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-A-009999-PPL1Y	$ 8.29	$ 7.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-A-009999-PPL2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-A-009999-PPL3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-A-009999-PPL4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 5,000-9999	RN-ETP-A-009999-PPL5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 5,000-9999	RN-ETP-A-009999-PTM1Y	$ 13.71	$ 11.93
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 5,000-9999	RN-ETP-A-009999-PTM2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 5,000-9999	RN-ETP-A-009999-PTM3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 5,000-9999	RN-ETP-A-009999-PTM4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 5,000-9999	RN-ETP-A-009999-PTM5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 5,000-9999	RN-ETP-A-009999-USG1Y	$ 14.75	$ 12.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 5,000-9999	RN-ETP-A-009999-USG2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 5,000-9999	RN-ETP-A-009999-USG3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 5,000-9999	RN-ETP-A-009999-USG4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 5,000-9999	RN-ETP-A-009999-USG5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-A-009999-USP1Y	$ 15.37	$ 13.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-A-009999-USP2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-A-009999-USP3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-A-009999-USP4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 5,000-9999	RN-ETP-A-009999-USP5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 10,000-19999	RN-ETP-A-019999-CAG1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 10,000-19999	RN-ETP-A-019999-CAG2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 10,000-19999	RN-ETP-A-019999-CAG3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 10,000-19999	RN-ETP-A-019999-CAG4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 10,000-19999	RN-ETP-A-019999-CAG5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 10,000-19999	RN-ETP-A-019999-CAP1Y	$ 13.44	$ 11.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 10,000-19999	RN-ETP-A-019999-CAP2Y	$ 25.13	$ 21.86

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 10,000-19999	RN-ETP-A-019999-CAP3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 10,000-19999	RN-ETP-A-019999-CAP4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 10,000-19999	RN-ETP-A-019999-CAP5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-A-019999-PPL1Y	$ 6.07	$ 5.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-A-019999-PPL2Y	$ 25.13	$ 21.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-A-019999-PPL3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-A-019999-PPL4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 10,000-19999	RN-ETP-A-019999-PPL5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 10,000-19999	RN-ETP-A-019999-PTM1Y	$ 10.79	$ 9.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 10,000-19999	RN-ETP-A-019999-PTM2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 10,000-19999	RN-ETP-A-019999-PTM3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 10,000-19999	RN-ETP-A-019999-PTM4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 10,000-19999	RN-ETP-A-019999-PTM5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 10,000-19999	RN-ETP-A-019999-USG1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 10,000-19999	RN-ETP-A-019999-USG2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 10,000-19999	RN-ETP-A-019999-USG3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 10,000-19999	RN-ETP-A-019999-USG4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 10,000-19999	RN-ETP-A-019999-USG5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-A-019999-USP1Y	$ 13.44	$ 11.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-A-019999-USP2Y	$ 25.13	$ 21.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-A-019999-USP3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-A-019999-USP4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 10,000-19999	RN-ETP-A-019999-USP5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 20,000-49999	RN-ETP-A-049999-CAG1Y	$ 11.55	$ 10.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 20,000-49999	RN-ETP-A-049999-CAG2Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 20,000-49999	RN-ETP-A-049999-CAG3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 20,000-49999	RN-ETP-A-049999-CAG4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 20,000-49999	RN-ETP-A-049999-CAG5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 20,000-49999	RN-ETP-A-049999-CAP1Y	$ 12.04	$ 10.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 20,000-49999	RN-ETP-A-049999-CAP2Y	$ 22.59	$ 19.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 20,000-49999	RN-ETP-A-049999-CAP3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 20,000-49999	RN-ETP-A-049999-CAP4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 20,000-49999	RN-ETP-A-049999-CAP5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-A-049999-PPL1Y	$ 4.85	$ 4.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-A-049999-PPL2Y	$ 22.50	$ 19.58
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-A-049999-PPL3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-A-049999-PPL4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 20,000-49999	RN-ETP-A-049999-PPL5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 20,000-49999	RN-ETP-A-049999-PTM1Y	$ 9.34	$ 8.13
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 20,000-49999	RN-ETP-A-049999-PTM2Y	$ 21.59	$ 18.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 20,000-49999	RN-ETP-A-049999-PTM3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 20,000-49999	RN-ETP-A-049999-PTM4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 20,000-49999	RN-ETP-A-049999-PTM5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 20,000-49999	RN-ETP-A-049999-USG1Y	$ 11.55	$ 10.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 20,000-49999	RN-ETP-A-049999-USG2Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 20,000-49999	RN-ETP-A-049999-USG3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 20,000-49999	RN-ETP-A-049999-USG4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 20,000-49999	RN-ETP-A-049999-USG5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-A-049999-USP1Y	$ 12.04	$ 10.47

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-A-049999-USP2Y	$ 22.59	$ 19.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-A-049999-USP3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-A-049999-USP4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 20,000-49999	RN-ETP-A-049999-USP5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 50,000-74999	RN-ETP-A-074999-CAG1Y	$ 11.84	$ 10.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 50,000-74999	RN-ETP-A-074999-CAG2Y	$ 22.18	$ 19.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 50,000-74999	RN-ETP-A-074999-CAG3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 50,000-74999	RN-ETP-A-074999-CAG4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 50,000-74999	RN-ETP-A-074999-CAG5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 50,000-74999	RN-ETP-A-074999-CAP1Y	$ 12.34	$ 10.74
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 50,000-74999	RN-ETP-A-074999-CAP2Y	$ 23.13	$ 20.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 50,000-74999	RN-ETP-A-074999-CAP3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 50,000-74999	RN-ETP-A-074999-CAP4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 50,000-74999	RN-ETP-A-074999-CAP5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-A-074999-PPL1Y	$ 4.76	$ 4.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-A-074999-PPL2Y	$ 23.06	$ 20.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-A-074999-PPL3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-A-074999-PPL4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 50,000-74999	RN-ETP-A-074999-PPL5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 50,000-74999	RN-ETP-A-074999-PTM1Y	$ 8.80	$ 7.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 50,000-74999	RN-ETP-A-074999-PTM2Y	$ 22.14	$ 19.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 50,000-74999	RN-ETP-A-074999-PTM3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 50,000-74999	RN-ETP-A-074999-PTM4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 50,000-74999	RN-ETP-A-074999-PTM5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 50,000-74999	RN-ETP-A-074999-USG1Y	$ 11.84	$ 10.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 50,000-74999	RN-ETP-A-074999-USG2Y	$ 22.18	$ 19.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 50,000-74999	RN-ETP-A-074999-USG3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 50,000-74999	RN-ETP-A-074999-USG4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 50,000-74999	RN-ETP-A-074999-USG5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-A-074999-USP1Y	$ 12.34	$ 10.74
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-A-074999-USP2Y	$ 23.13	$ 20.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-A-074999-USP3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-A-074999-USP4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 50,000-74999	RN-ETP-A-074999-USP5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 75,000-99999	RN-ETP-A-099999-CAG1Y	$ 12.39	$ 10.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 75,000-99999	RN-ETP-A-099999-CAG2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 75,000-99999	RN-ETP-A-099999-CAG3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 75,000-99999	RN-ETP-A-099999-CAG4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 75,000-99999	RN-ETP-A-099999-CAG5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 75,000-99999	RN-ETP-A-099999-CAP1Y	$ 12.91	$ 11.23
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 75,000-99999	RN-ETP-A-099999-CAP2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 75,000-99999	RN-ETP-A-099999-CAP3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 75,000-99999	RN-ETP-A-099999-CAP4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 75,000-99999	RN-ETP-A-099999-CAP5Y	$ 58.10	$ 50.55
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-A-099999-PPL1Y	$ 4.76	$ 4.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-A-099999-PPL2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-A-099999-PPL3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-A-099999-PPL4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 75,000-99999	RN-ETP-A-099999-PPL5Y	$ 58.10	$ 50.55

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 75,000-99999	RN-ETP-A-099999-PTM1Y	$ 8.22	$ 7.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 75,000-99999	RN-ETP-A-099999-PTM2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 75,000-99999	RN-ETP-A-099999-PTM3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 75,000-99999	RN-ETP-A-099999-PTM4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 75,000-99999	RN-ETP-A-099999-PTM5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 75,000-99999	RN-ETP-A-099999-USG1Y	$ 12.39	$ 10.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 75,000-99999	RN-ETP-A-099999-USG2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 75,000-99999	RN-ETP-A-099999-USG3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 75,000-99999	RN-ETP-A-099999-USG4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 75,000-99999	RN-ETP-A-099999-USG5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-A-099999-USP1Y	$ 12.91	$ 11.23
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-A-099999-USP2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-A-099999-USP3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-A-099999-USP4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 75,000-99999	RN-ETP-A-099999-USP5Y	$ 58.10	$ 50.55
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 100,000-199999	RN-ETP-A-199999-CAG1Y	$ 10.78	$ 9.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 100,000-199999	RN-ETP-A-199999-CAG2Y	$ 20.15	$ 17.53
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 100,000-199999	RN-ETP-A-199999-CAG3Y	$ 29.11	$ 25.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 100,000-199999	RN-ETP-A-199999-CAG4Y	$ 38.81	$ 33.76
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 100,000-199999	RN-ETP-A-199999-CAG5Y	$ 48.51	$ 42.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 100,000-199999	RN-ETP-A-199999-CAP1Y	$ 11.23	$ 9.77
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 100,000-199999	RN-ETP-A-199999-CAP2Y	$ 21.01	$ 18.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 100,000-199999	RN-ETP-A-199999-CAP3Y	$ 30.32	$ 26.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 100,000-199999	RN-ETP-A-199999-CAP4Y	$ 40.43	$ 35.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 100,000-199999	RN-ETP-A-199999-CAP5Y	$ 50.54	$ 43.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-A-199999-PPL1Y	$ 3.50	$ 3.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-A-199999-PPL2Y	$ 21.09	$ 18.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-A-199999-PPL3Y	$ 30.48	$ 26.52
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-A-199999-PPL4Y	$ 40.64	$ 35.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 100,000-199999	RN-ETP-A-199999-PPL5Y	$ 50.81	$ 44.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 100,000-199999	RN-ETP-A-199999-PTM1Y	$ 6.58	$ 5.72
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 100,000-199999	RN-ETP-A-199999-PTM2Y	$ 20.25	$ 17.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 100,000-199999	RN-ETP-A-199999-PTM3Y	$ 29.24	$ 25.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 100,000-199999	RN-ETP-A-199999-PTM4Y	$ 38.99	$ 33.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 100,000-199999	RN-ETP-A-199999-PTM5Y	$ 48.74	$ 42.40
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 100,000-199999	RN-ETP-A-199999-USG1Y	$ 10.78	$ 9.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 100,000-199999	RN-ETP-A-199999-USG2Y	$ 20.15	$ 17.53
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 100,000-199999	RN-ETP-A-199999-USG3Y	$ 29.11	$ 25.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 100,000-199999	RN-ETP-A-199999-USG4Y	$ 38.81	$ 33.76
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 100,000-199999	RN-ETP-A-199999-USG5Y	$ 48.51	$ 42.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-A-199999-USP1Y	$ 11.23	$ 9.77
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-A-199999-USP2Y	$ 21.01	$ 18.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-A-199999-USP3Y	$ 30.32	$ 26.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-A-199999-USP4Y	$ 40.43	$ 35.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 100,000-199999	RN-ETP-A-199999-USP5Y	$ 50.54	$ 43.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 200,000+	RN-ETP-A-200000+CAG1Y	$ 10.42	$ 9.07
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 200,000+	RN-ETP-A-200000+CAG2Y	$ 19.49	$ 16.96
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 200,000+	RN-ETP-A-200000+CAG3Y	$ 28.13	$ 24.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 200,000+	RN-ETP-A-200000+CAG4Y	$ 37.51	$ 32.63

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 200,000+	RN-ETP-A-200000+CAG5Y	$ 46.89	$ 40.79
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 200,000+	RN-ETP-A-200000+CAP1Y	$ 10.86	$ 9.45
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 200,000+	RN-ETP-A-200000+CAP2Y	$ 20.30	$ 17.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 200,000+	RN-ETP-A-200000+CAP3Y	$ 29.32	$ 25.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 200,000+	RN-ETP-A-200000+CAP4Y	$ 39.10	$ 34.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 200,000+	RN-ETP-A-200000+CAP5Y	$ 48.87	$ 42.52
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 200,000+	RN-ETP-A-200000+PPL1Y	$ 3.13	$ 2.72
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 200,000+	RN-ETP-A-200000+PPL2Y	$ 20.32	$ 17.68
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 200,000+	RN-ETP-A-200000+PPL3Y	$ 29.38	$ 25.56
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 200,000+	RN-ETP-A-200000+PPL4Y	$ 39.17	$ 34.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 200,000+	RN-ETP-A-200000+PPL5Y	$ 48.96	$ 42.60
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 200,000+	RN-ETP-A-200000+PTM1Y	$ 6.04	$ 5.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 200,000+	RN-ETP-A-200000+PTM2Y	$ 19.51	$ 16.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 200,000+	RN-ETP-A-200000+PTM3Y	$ 28.16	$ 24.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 200,000+	RN-ETP-A-200000+PTM4Y	$ 37.55	$ 32.67
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 200,000+	RN-ETP-A-200000+PTM5Y	$ 46.94	$ 40.84
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 200,000+	RN-ETP-A-200000+USG1Y	$ 10.42	$ 9.07
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 200,000+	RN-ETP-A-200000+USG2Y	$ 19.49	$ 16.96
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 200,000+	RN-ETP-A-200000+USG3Y	$ 28.13	$ 24.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 200,000+	RN-ETP-A-200000+USG4Y	$ 37.51	$ 32.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 200,000+	RN-ETP-A-200000+USG5Y	$ 46.89	$ 40.79
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-A-200000+USP1Y	$ 10.86	$ 9.45
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-A-200000+USP2Y	$ 20.30	$ 17.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-A-200000+USP3Y	$ 29.32	$ 25.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-A-200000+USP4Y	$ 39.10	$ 34.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 200,000+	RN-ETP-A-200000+USP5Y	$ 48.87	$ 42.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1-249	RN-ETP-C-000249-CAG1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1-249	RN-ETP-C-000249-CAG2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1-249	RN-ETP-C-000249-CAG3Y	$ 228.31	$ 198.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1-249	RN-ETP-C-000249-CAG4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1-249	RN-ETP-C-000249-CAG5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1-249	RN-ETP-C-000249-CAP1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1-249	RN-ETP-C-000249-CAP2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1-249	RN-ETP-C-000249-CAP3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1-249	RN-ETP-C-000249-CAP4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1-249	RN-ETP-C-000249-CAP5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1-249	RN-ETP-C-000249-PPL1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1-249	RN-ETP-C-000249-PPL2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1-249	RN-ETP-C-000249-PPL3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1-249	RN-ETP-C-000249-PPL4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1-249	RN-ETP-C-000249-PPL5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1-249	RN-ETP-C-000249-PTM1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1-249	RN-ETP-C-000249-PTM2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1-249	RN-ETP-C-000249-PTM3Y	$ 228.31	$ 198.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1-249	RN-ETP-C-000249-PTM4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1-249	RN-ETP-C-000249-PTM5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1-249	RN-ETP-C-000249-USG1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1-249	RN-ETP-C-000249-USG2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1-249	RN-ETP-C-000249-USG3Y	$ 228.31	$ 198.63

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1-249	RN-ETP-C-000249-USG4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1-249	RN-ETP-C-000249-USG5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-C-000249-USP1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-C-000249-USP2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-C-000249-USP3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-C-000249-USP4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1-249	RN-ETP-C-000249-USP5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 250-499	RN-ETP-C-000499-CAG1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 250-499	RN-ETP-C-000499-CAG2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 250-499	RN-ETP-C-000499-CAG3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 250-499	RN-ETP-C-000499-CAG4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 250-499	RN-ETP-C-000499-CAG5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 250-499	RN-ETP-C-000499-CAP1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 250-499	RN-ETP-C-000499-CAP2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 250-499	RN-ETP-C-000499-CAP3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 250-499	RN-ETP-C-000499-CAP4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 250-499	RN-ETP-C-000499-CAP5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 250-499	RN-ETP-C-000499-PPL1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 250-499	RN-ETP-C-000499-PPL2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 250-499	RN-ETP-C-000499-PPL3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 250-499	RN-ETP-C-000499-PPL4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 250-499	RN-ETP-C-000499-PPL5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 250-499	RN-ETP-C-000499-PTM1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 250-499	RN-ETP-C-000499-PTM2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 250-499	RN-ETP-C-000499-PTM3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 250-499	RN-ETP-C-000499-PTM4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 250-499	RN-ETP-C-000499-PTM5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 250-499	RN-ETP-C-000499-USG1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 250-499	RN-ETP-C-000499-USG2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 250-499	RN-ETP-C-000499-USG3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 250-499	RN-ETP-C-000499-USG4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 250-499	RN-ETP-C-000499-USG5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-C-000499-USP1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-C-000499-USP2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-C-000499-USP3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-C-000499-USP4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 250-499	RN-ETP-C-000499-USP5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 500-749	RN-ETP-C-000749-CAG1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 500-749	RN-ETP-C-000749-CAG2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 500-749	RN-ETP-C-000749-CAG3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 500-749	RN-ETP-C-000749-CAG4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 500-749	RN-ETP-C-000749-CAG5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 500-749	RN-ETP-C-000749-CAP1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 500-749	RN-ETP-C-000749-CAP2Y	$ 124.86	$ 108.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 500-749	RN-ETP-C-000749-CAP3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 500-749	RN-ETP-C-000749-CAP4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 500-749	RN-ETP-C-000749-CAP5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 500-749	RN-ETP-C-000749-PPL1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 500-749	RN-ETP-C-000749-PPL2Y	$ 124.86	$ 108.63

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 500-749	RN-ETP-C-000749-PPL3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 500-749	RN-ETP-C-000749-PPL4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 500-749	RN-ETP-C-000749-PPL5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 500-749	RN-ETP-C-000749-PTM1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 500-749	RN-ETP-C-000749-PTM2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 500-749	RN-ETP-C-000749-PTM3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 500-749	RN-ETP-C-000749-PTM4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 500-749	RN-ETP-C-000749-PTM5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 500-749	RN-ETP-C-000749-USG1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 500-749	RN-ETP-C-000749-USG2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 500-749	RN-ETP-C-000749-USG3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 500-749	RN-ETP-C-000749-USG4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 500-749	RN-ETP-C-000749-USG5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-C-000749-USP1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-C-000749-USP2Y	$ 124.86	$ 108.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-C-000749-USP3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-C-000749-USP4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 500-749	RN-ETP-C-000749-USP5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 750-999	RN-ETP-C-000999-CAG1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 750-999	RN-ETP-C-000999-CAG2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 750-999	RN-ETP-C-000999-CAG3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 750-999	RN-ETP-C-000999-CAG4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 750-999	RN-ETP-C-000999-CAG5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 750-999	RN-ETP-C-000999-CAP1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 750-999	RN-ETP-C-000999-CAP2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 750-999	RN-ETP-C-000999-CAP3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 750-999	RN-ETP-C-000999-CAP4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 750-999	RN-ETP-C-000999-CAP5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 750-999	RN-ETP-C-000999-PPL1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 750-999	RN-ETP-C-000999-PPL2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 750-999	RN-ETP-C-000999-PPL3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 750-999	RN-ETP-C-000999-PPL4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 750-999	RN-ETP-C-000999-PPL5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 750-999	RN-ETP-C-000999-PTM1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 750-999	RN-ETP-C-000999-PTM2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 750-999	RN-ETP-C-000999-PTM3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 750-999	RN-ETP-C-000999-PTM4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 750-999	RN-ETP-C-000999-PTM5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 750-999	RN-ETP-C-000999-USG1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 750-999	RN-ETP-C-000999-USG2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 750-999	RN-ETP-C-000999-USG3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 750-999	RN-ETP-C-000999-USG4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 750-999	RN-ETP-C-000999-USG5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-C-000999-USP1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-C-000999-USP2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-C-000999-USP3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-C-000999-USP4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 750-999	RN-ETP-C-000999-USP5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1,000-1999	RN-ETP-C-001999-CAG1Y	$ 45.62	$ 39.69

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1,000-1999	RN-ETP-C-001999-CAG2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1,000-1999	RN-ETP-C-001999-CAG3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1,000-1999	RN-ETP-C-001999-CAG4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1,000-1999	RN-ETP-C-001999-CAG5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1,000-1999	RN-ETP-C-001999-CAP1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1,000-1999	RN-ETP-C-001999-CAP2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1,000-1999	RN-ETP-C-001999-CAP3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1,000-1999	RN-ETP-C-001999-CAP4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1,000-1999	RN-ETP-C-001999-CAP5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-C-001999-PPL1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-C-001999-PPL2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-C-001999-PPL3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-C-001999-PPL4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1,000-1999	RN-ETP-C-001999-PPL5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1,000-1999	RN-ETP-C-001999-PTM1Y	$ 45.62	$ 39.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1,000-1999	RN-ETP-C-001999-PTM2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1,000-1999	RN-ETP-C-001999-PTM3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1,000-1999	RN-ETP-C-001999-PTM4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1,000-1999	RN-ETP-C-001999-PTM5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1,000-1999	RN-ETP-C-001999-USG1Y	$ 45.62	$ 39.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1,000-1999	RN-ETP-C-001999-USG2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1,000-1999	RN-ETP-C-001999-USG3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1,000-1999	RN-ETP-C-001999-USG4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1,000-1999	RN-ETP-C-001999-USG5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-C-001999-USP1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-C-001999-USP2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-C-001999-USP3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-C-001999-USP4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1,000-1999	RN-ETP-C-001999-USP5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 2,000-4999	RN-ETP-C-004999-CAG1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 2,000-4999	RN-ETP-C-004999-CAG2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 2,000-4999	RN-ETP-C-004999-CAG3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 2,000-4999	RN-ETP-C-004999-CAG4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 2,000-4999	RN-ETP-C-004999-CAG5Y	$ 186.89	$ 162.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 2,000-4999	RN-ETP-C-004999-CAP1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 2,000-4999	RN-ETP-C-004999-CAP2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 2,000-4999	RN-ETP-C-004999-CAP3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 2,000-4999	RN-ETP-C-004999-CAP4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 2,000-4999	RN-ETP-C-004999-CAP5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-C-004999-PPL1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-C-004999-PPL2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-C-004999-PPL3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-C-004999-PPL4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 2,000-4999	RN-ETP-C-004999-PPL5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 2,000-4999	RN-ETP-C-004999-PTM1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 2,000-4999	RN-ETP-C-004999-PTM2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 2,000-4999	RN-ETP-C-004999-PTM3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 2,000-4999	RN-ETP-C-004999-PTM4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 2,000-4999	RN-ETP-C-004999-PTM5Y	$ 186.89	$ 162.59

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 2,000-4999	RN-ETP-C-004999-USG1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 2,000-4999	RN-ETP-C-004999-USG2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 2,000-4999	RN-ETP-C-004999-USG3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 2,000-4999	RN-ETP-C-004999-USG4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 2,000-4999	RN-ETP-C-004999-USG5Y	$ 186.89	$ 162.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-C-004999-USP1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-C-004999-USP2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-C-004999-USP3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-C-004999-USP4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 2,000-4999	RN-ETP-C-004999-USP5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 5,000-9999	RN-ETP-C-009999-CAG1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 5,000-9999	RN-ETP-C-009999-CAG2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 5,000-9999	RN-ETP-C-009999-CAG3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 5,000-9999	RN-ETP-C-009999-CAG4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 5,000-9999	RN-ETP-C-009999-CAG5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 5,000-9999	RN-ETP-C-009999-CAP1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 5,000-9999	RN-ETP-C-009999-CAP2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 5,000-9999	RN-ETP-C-009999-CAP3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 5,000-9999	RN-ETP-C-009999-CAP4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 5,000-9999	RN-ETP-C-009999-CAP5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-C-009999-PPL1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-C-009999-PPL2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-C-009999-PPL3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-C-009999-PPL4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 5,000-9999	RN-ETP-C-009999-PPL5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 5,000-9999	RN-ETP-C-009999-PTM1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 5,000-9999	RN-ETP-C-009999-PTM2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 5,000-9999	RN-ETP-C-009999-PTM3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 5,000-9999	RN-ETP-C-009999-PTM4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 5,000-9999	RN-ETP-C-009999-PTM5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 5,000-9999	RN-ETP-C-009999-USG1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 5,000-9999	RN-ETP-C-009999-USG2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 5,000-9999	RN-ETP-C-009999-USG3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 5,000-9999	RN-ETP-C-009999-USG4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 5,000-9999	RN-ETP-C-009999-USG5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-C-009999-USP1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-C-009999-USP2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-C-009999-USP3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-C-009999-USP4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 5,000-9999	RN-ETP-C-009999-USP5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 10,000-19999	RN-ETP-C-019999-CAG1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 10,000-19999	RN-ETP-C-019999-CAG2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 10,000-19999	RN-ETP-C-019999-CAG3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 10,000-19999	RN-ETP-C-019999-CAG4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 10,000-19999	RN-ETP-C-019999-CAG5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 10,000-19999	RN-ETP-C-019999-CAP1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 10,000-19999	RN-ETP-C-019999-CAP2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 10,000-19999	RN-ETP-C-019999-CAP3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 10,000-19999	RN-ETP-C-019999-CAP4Y	$ 123.12	$ 107.11

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 10,000-19999	RN-ETP-C-019999-CAP5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-C-019999-PPL1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-C-019999-PPL2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-C-019999-PPL3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-C-019999-PPL4Y	$ 123.12	$ 107.11
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 10,000-19999	RN-ETP-C-019999-PPL5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 10,000-19999	RN-ETP-C-019999-PTM1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 10,000-19999	RN-ETP-C-019999-PTM2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 10,000-19999	RN-ETP-C-019999-PTM3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 10,000-19999	RN-ETP-C-019999-PTM4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 10,000-19999	RN-ETP-C-019999-PTM5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 10,000-19999	RN-ETP-C-019999-USG1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 10,000-19999	RN-ETP-C-019999-USG2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 10,000-19999	RN-ETP-C-019999-USG3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 10,000-19999	RN-ETP-C-019999-USG4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 10,000-19999	RN-ETP-C-019999-USG5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-C-019999-USP1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-C-019999-USP2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-C-019999-USP3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-C-019999-USP4Y	$ 123.12	$ 107.11
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 10,000-19999	RN-ETP-C-019999-USP5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 20,000-49999	RN-ETP-C-049999-CAG1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 20,000-49999	RN-ETP-C-049999-CAG2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 20,000-49999	RN-ETP-C-049999-CAG3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 20,000-49999	RN-ETP-C-049999-CAG4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 20,000-49999	RN-ETP-C-049999-CAG5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 20,000-49999	RN-ETP-C-049999-CAP1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 20,000-49999	RN-ETP-C-049999-CAP2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 20,000-49999	RN-ETP-C-049999-CAP3Y	$ 84.73	$ 73.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 20,000-49999	RN-ETP-C-049999-CAP4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 20,000-49999	RN-ETP-C-049999-CAP5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-C-049999-PPL1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-C-049999-PPL2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-C-049999-PPL3Y	$ 84.73	$ 73.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-C-049999-PPL4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 20,000-49999	RN-ETP-C-049999-PPL5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 20,000-49999	RN-ETP-C-049999-PTM1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 20,000-49999	RN-ETP-C-049999-PTM2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 20,000-49999	RN-ETP-C-049999-PTM3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 20,000-49999	RN-ETP-C-049999-PTM4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 20,000-49999	RN-ETP-C-049999-PTM5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 20,000-49999	RN-ETP-C-049999-USG1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 20,000-49999	RN-ETP-C-049999-USG2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 20,000-49999	RN-ETP-C-049999-USG3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 20,000-49999	RN-ETP-C-049999-USG4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 20,000-49999	RN-ETP-C-049999-USG5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-C-049999-USP1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-C-049999-USP2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-C-049999-USP3Y	$ 84.73	$ 73.72

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-C-049999-USP4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 20,000-49999	RN-ETP-C-049999-USP5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 50,000-74999	RN-ETP-C-074999-CAG1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 50,000-74999	RN-ETP-C-074999-CAG2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 50,000-74999	RN-ETP-C-074999-CAG3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 50,000-74999	RN-ETP-C-074999-CAG4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 50,000-74999	RN-ETP-C-074999-CAG5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 50,000-74999	RN-ETP-C-074999-CAP1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 50,000-74999	RN-ETP-C-074999-CAP2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 50,000-74999	RN-ETP-C-074999-CAP3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 50,000-74999	RN-ETP-C-074999-CAP4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 50,000-74999	RN-ETP-C-074999-CAP5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-C-074999-PPL1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-C-074999-PPL2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-C-074999-PPL3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-C-074999-PPL4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 50,000-74999	RN-ETP-C-074999-PPL5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 50,000-74999	RN-ETP-C-074999-PTM1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 50,000-74999	RN-ETP-C-074999-PTM2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 50,000-74999	RN-ETP-C-074999-PTM3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 50,000-74999	RN-ETP-C-074999-PTM4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 50,000-74999	RN-ETP-C-074999-PTM5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 50,000-74999	RN-ETP-C-074999-USG1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 50,000-74999	RN-ETP-C-074999-USG2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 50,000-74999	RN-ETP-C-074999-USG3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 50,000-74999	RN-ETP-C-074999-USG4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 50,000-74999	RN-ETP-C-074999-USG5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-C-074999-USP1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-C-074999-USP2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-C-074999-USP3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-C-074999-USP4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 50,000-74999	RN-ETP-C-074999-USP5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 75,000-99999	RN-ETP-C-099999-CAG1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 75,000-99999	RN-ETP-C-099999-CAG2Y	$ 48.88	$ 42.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 75,000-99999	RN-ETP-C-099999-CAG3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 75,000-99999	RN-ETP-C-099999-CAG4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 75,000-99999	RN-ETP-C-099999-CAG5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 75,000-99999	RN-ETP-C-099999-CAP1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 75,000-99999	RN-ETP-C-099999-CAP2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 75,000-99999	RN-ETP-C-099999-CAP3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 75,000-99999	RN-ETP-C-099999-CAP4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 75,000-99999	RN-ETP-C-099999-CAP5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-C-099999-PPL1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-C-099999-PPL2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-C-099999-PPL3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-C-099999-PPL4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 75,000-99999	RN-ETP-C-099999-PPL5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 75,000-99999	RN-ETP-C-099999-PTM1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 75,000-99999	RN-ETP-C-099999-PTM2Y	$ 48.88	$ 42.53

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 75,000-99999	RN-ETP-C-099999-PTM3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 75,000-99999	RN-ETP-C-099999-PTM4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 75,000-99999	RN-ETP-C-099999-PTM5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 75,000-99999	RN-ETP-C-099999-USG1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 75,000-99999	RN-ETP-C-099999-USG2Y	$ 48.88	$ 42.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 75,000-99999	RN-ETP-C-099999-USG3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 75,000-99999	RN-ETP-C-099999-USG4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 75,000-99999	RN-ETP-C-099999-USG5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-C-099999-USP1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-C-099999-USP2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-C-099999-USP3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-C-099999-USP4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 75,000-99999	RN-ETP-C-099999-USP5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 100,000-199999	RN-ETP-C-199999-CAG1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 100,000-199999	RN-ETP-C-199999-CAG2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 100,000-199999	RN-ETP-C-199999-CAG3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 100,000-199999	RN-ETP-C-199999-CAG4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 100,000-199999	RN-ETP-C-199999-CAG5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 100,000-199999	RN-ETP-C-199999-CAP1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 100,000-199999	RN-ETP-C-199999-CAP2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 100,000-199999	RN-ETP-C-199999-CAP3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 100,000-199999	RN-ETP-C-199999-CAP4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 100,000-199999	RN-ETP-C-199999-CAP5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-C-199999-PPL1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-C-199999-PPL2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-C-199999-PPL3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-C-199999-PPL4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 100,000-199999	RN-ETP-C-199999-PPL5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 100,000-199999	RN-ETP-C-199999-PTM1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 100,000-199999	RN-ETP-C-199999-PTM2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 100,000-199999	RN-ETP-C-199999-PTM3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 100,000-199999	RN-ETP-C-199999-PTM4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 100,000-199999	RN-ETP-C-199999-PTM5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 100,000-199999	RN-ETP-C-199999-USG1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 100,000-199999	RN-ETP-C-199999-USG2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 100,000-199999	RN-ETP-C-199999-USG3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 100,000-199999	RN-ETP-C-199999-USG4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 100,000-199999	RN-ETP-C-199999-USG5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-C-199999-USP1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-C-199999-USP2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-C-199999-USP3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-C-199999-USP4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 100,000-199999	RN-ETP-C-199999-USP5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 200,000+	RN-ETP-C-200000+CAG1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 200,000+	RN-ETP-C-200000+CAG2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 200,000+	RN-ETP-C-200000+CAG3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 200,000+	RN-ETP-C-200000+CAG4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 200,000+	RN-ETP-C-200000+CAG5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 200,000+	RN-ETP-C-200000+CAP1Y	$ 20.33	$ 17.69

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 200,000+	RN-ETP-C-200000+CAP2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 200,000+	RN-ETP-C-200000+CAP3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 200,000+	RN-ETP-C-200000+CAP4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 200,000+	RN-ETP-C-200000+CAP5Y	$ 91.49	$ 79.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 200,000+	RN-ETP-C-200000+PPL1Y	$ 20.33	$ 17.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 200,000+	RN-ETP-C-200000+PPL2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 200,000+	RN-ETP-C-200000+PPL3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 200,000+	RN-ETP-C-200000+PPL4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 200,000+	RN-ETP-C-200000+PPL5Y	$ 91.49	$ 79.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 200,000+	RN-ETP-C-200000+PTM1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 200,000+	RN-ETP-C-200000+PTM2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 200,000+	RN-ETP-C-200000+PTM3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 200,000+	RN-ETP-C-200000+PTM4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 200,000+	RN-ETP-C-200000+PTM5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 200,000+	RN-ETP-C-200000+USG1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 200,000+	RN-ETP-C-200000+USG2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 200,000+	RN-ETP-C-200000+USG3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 200,000+	RN-ETP-C-200000+USG4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 200,000+	RN-ETP-C-200000+USG5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-C-200000+USP1Y	$ 20.33	$ 17.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-C-200000+USP2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-C-200000+USP3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-C-200000+USP4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 200,000+	RN-ETP-C-200000+USP5Y	$ 91.49	$ 79.60
FireEye	Online Web Training-30-day access to eLearning, self-paced, course on Email Threat Prevention Cloud Deployment	EDU-OWT-BSC-ETP	$ 295.00	$ 256.65
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 1-249	ETP-000249-PPL1Y	$ 74.52	$ 64.83
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 1-249	ETP-000249-PPL2Y	$ 149.04	$ 129.66
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 1-249	ETP-000249-PPL3Y	$ 201.20	$ 175.04
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 1-249	ETP-000249-PPL4Y	$ 268.27	$ 233.39
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 1-249	ETP-000249-PPL5Y	$ 335.34	$ 291.75
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1-249	ETP-000249-USP1Y	$ 74.52	$ 64.83
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1-249	ETP-000249-USP2Y	$ 149.04	$ 129.66
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1-249	ETP-000249-USP3Y	$ 201.20	$ 175.04
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1-249	ETP-000249-USP4Y	$ 268.27	$ 233.39
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 1-249	ETP-000249-USP5Y	$ 335.34	$ 291.75
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 250-499	ETP-000499-PPL1Y	$ 61.52	$ 53.52
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 250-499	ETP-000499-PPL2Y	$ 123.04	$ 107.04
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 250-499	ETP-000499-PPL3Y	$ 166.10	$ 144.51
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 250-499	ETP-000499-PPL4Y	$ 221.47	$ 192.68
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 250-499	ETP-000499-PPL5Y	$ 276.84	$ 240.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 250-499	ETP-000499-USP1Y	$ 61.52	$ 53.52
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 250-499	ETP-000499-USP2Y	$ 123.04	$ 107.04
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 250-499	ETP-000499-USP3Y	$ 166.10	$ 144.51
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 250-499	ETP-000499-USP4Y	$ 221.47	$ 192.68
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 250-499	ETP-000499-USP5Y	$ 276.84	$ 240.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 500-749	ETP-000749-PPL1Y	$ 52.77	$ 45.91
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 500-749	ETP-000749-PPL2Y	$ 105.54	$ 91.82
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 500-749	ETP-000749-PPL3Y	$ 142.48	$ 123.96
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 500-749	ETP-000749-PPL4Y	$ 189.97	$ 165.27

FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 500-749	ETP-000749-PPL5Y	$ 237.47	$ 206.60
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 500-749	ETP-000749-USP1Y	$ 52.77	$ 45.91
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 500-749	ETP-000749-USP2Y	$ 105.54	$ 91.82
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 500-749	ETP-000749-USP3Y	$ 142.48	$ 123.96
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 500-749	ETP-000749-USP4Y	$ 189.97	$ 165.27
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 500-749	ETP-000749-USP5Y	$ 237.47	$ 206.60
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 750-999	ETP-000999-PPL1Y	$ 44.32	$ 38.56
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 750-999	ETP-000999-PPL2Y	$ 88.64	$ 77.12
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 750-999	ETP-000999-PPL3Y	$ 119.66	$ 104.10
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 750-999	ETP-000999-PPL4Y	$ 159.55	$ 138.81
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 750-999	ETP-000999-PPL5Y	$ 199.44	$ 173.51
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 750-999	ETP-000999-USP1Y	$ 44.32	$ 38.56
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 750-999	ETP-000999-USP2Y	$ 88.64	$ 77.12
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 750-999	ETP-000999-USP3Y	$ 119.66	$ 104.10
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 750-999	ETP-000999-USP4Y	$ 159.55	$ 138.81
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 750-999	ETP-000999-USP5Y	$ 199.44	$ 173.51
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 1,000-1999	ETP-001999-PPL1Y	$ 40.20	$ 34.97
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 1,000-1999	ETP-001999-PPL2Y	$ 80.40	$ 69.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 1,000-1999	ETP-001999-PPL3Y	$ 108.54	$ 94.43
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 1,000-1999	ETP-001999-PPL4Y	$ 144.72	$ 125.91
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 1,000-1999	ETP-001999-PPL5Y	$ 180.90	$ 157.38
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-001999-USP1Y	$ 40.20	$ 34.97
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-001999-USP2Y	$ 80.40	$ 69.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-001999-USP3Y	$ 108.54	$ 94.43
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-001999-USP4Y	$ 144.72	$ 125.91
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-001999-USP5Y	$ 180.90	$ 157.38
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 2,000-4999	ETP-004999-PPL1Y	$ 36.59	$ 31.83
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 2,000-4999	ETP-004999-PPL2Y	$ 73.18	$ 63.67
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 2,000-4999	ETP-004999-PPL3Y	$ 98.79	$ 85.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 2,000-4999	ETP-004999-PPL4Y	$ 131.72	$ 114.60
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 2,000-4999	ETP-004999-PPL5Y	$ 164.66	$ 143.25
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-004999-USP1Y	$ 36.59	$ 31.83
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-004999-USP2Y	$ 73.18	$ 63.67
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-004999-USP3Y	$ 98.79	$ 85.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-004999-USP4Y	$ 131.72	$ 114.60
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-004999-USP5Y	$ 164.66	$ 143.25
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 5,000-9999	ETP-009999-PPL1Y	$ 32.59	$ 28.35
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 5,000-9999	ETP-009999-PPL2Y	$ 65.18	$ 56.71
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 5,000-9999	ETP-009999-PPL3Y	$ 87.99	$ 76.55
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 5,000-9999	ETP-009999-PPL4Y	$ 117.32	$ 102.07
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 5,000-9999	ETP-009999-PPL5Y	$ 146.66	$ 127.59
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-009999-USP1Y	$ 32.59	$ 28.35
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-009999-USP2Y	$ 65.18	$ 56.71
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-009999-USP3Y	$ 87.99	$ 76.55
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-009999-USP4Y	$ 117.32	$ 102.07
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-009999-USP5Y	$ 146.66	$ 127.59
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 10,000-19999	ETP-019999-PPL1Y	$ 28.13	$ 24.47
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 10,000-19999	ETP-019999-PPL2Y	$ 56.26	$ 48.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 10,000-19999	ETP-019999-PPL3Y	$ 75.95	$ 66.08

FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 10,000-19999	ETP-019999-PPL4Y	$ 101.27	$ 88.10
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 10,000-19999	ETP-019999-PPL5Y	$ 126.59	$ 110.13
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-019999-USP1Y	$ 28.13	$ 24.47
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-019999-USP2Y	$ 56.26	$ 48.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-019999-USP3Y	$ 75.95	$ 66.08
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-019999-USP4Y	$ 101.27	$ 88.10
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-019999-USP5Y	$ 126.59	$ 110.13
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 20,000-49999	ETP-049999-PPL1Y	$ 26.53	$ 23.08
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 20,000-49999	ETP-049999-PPL2Y	$ 53.06	$ 46.16
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 20,000-49999	ETP-049999-PPL3Y	$ 71.63	$ 62.32
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 20,000-49999	ETP-049999-PPL4Y	$ 95.51	$ 83.09
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 20,000-49999	ETP-049999-PPL5Y	$ 119.39	$ 103.87
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-049999-USP1Y	$ 26.53	$ 23.08
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-049999-USP2Y	$ 53.06	$ 46.16
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-049999-USP3Y	$ 71.63	$ 62.32
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-049999-USP4Y	$ 95.51	$ 83.09
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-049999-USP5Y	$ 119.39	$ 103.87
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 50,000-74999	ETP-074999-PPL1Y	$ 23.96	$ 20.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 50,000-74999	ETP-074999-PPL2Y	$ 47.92	$ 41.69
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 50,000-74999	ETP-074999-PPL3Y	$ 64.69	$ 56.28
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 50,000-74999	ETP-074999-PPL4Y	$ 86.26	$ 75.05
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 50,000-74999	ETP-074999-PPL5Y	$ 107.82	$ 93.80
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-074999-USP1Y	$ 23.96	$ 20.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-074999-USP2Y	$ 47.92	$ 41.69
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-074999-USP3Y	$ 64.69	$ 56.28
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-074999-USP4Y	$ 86.26	$ 75.05
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-074999-USP5Y	$ 107.82	$ 93.80
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 75,000-99999	ETP-099999-PPL1Y	$ 20.72	$ 18.03
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 75,000-99999	ETP-099999-PPL2Y	$ 41.44	$ 36.05
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 75,000-99999	ETP-099999-PPL3Y	$ 55.94	$ 48.67
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 75,000-99999	ETP-099999-PPL4Y	$ 74.59	$ 64.89
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 75,000-99999	ETP-099999-PPL5Y	$ 93.24	$ 81.12
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-099999-USP1Y	$ 20.72	$ 18.03
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-099999-USP2Y	$ 41.44	$ 36.05
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-099999-USP3Y	$ 55.94	$ 48.67
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-099999-USP4Y	$ 74.59	$ 64.89
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-099999-USP5Y	$ 93.24	$ 81.12
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 100,000-199999	ETP-199999-PPL1Y	$ 18.22	$ 15.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 100,000-199999	ETP-199999-PPL2Y	$ 36.44	$ 31.70
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 100,000-199999	ETP-199999-PPL3Y	$ 49.19	$ 42.80
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 100,000-199999	ETP-199999-PPL4Y	$ 65.59	$ 57.06
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 100,000-199999	ETP-199999-PPL5Y	$ 81.99	$ 71.33
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-199999-USP1Y	$ 18.22	$ 15.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-199999-USP2Y	$ 36.44	$ 31.70
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-199999-USP3Y	$ 49.19	$ 42.80
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-199999-USP4Y	$ 65.59	$ 57.06
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-199999-USP5Y	$ 81.99	$ 71.33
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 200,000+	ETP-200000+PPL1Y	$ 17.20	$ 14.96
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 200,000+	ETP-200000+PPL2Y	$ 34.40	$ 29.93

FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 200,000+	ETP-200000+PPL3Y	$ 46.44	$ 40.40
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 200,000+	ETP-200000+PPL4Y	$ 61.92	$ 53.87
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 200,000+	ETP-200000+PPL5Y	$ 77.40	$ 67.34
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 200,000+	ETP-200000+USP1Y	$ 17.20	$ 14.96
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 200,000+	ETP-200000+USP2Y	$ 34.40	$ 29.93
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 200,000+	ETP-200000+USP3Y	$ 46.44	$ 40.40
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 200,000+	ETP-200000+USP4Y	$ 61.92	$ 53.87
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 200,000+	ETP-200000+USP5Y	$ 77.40	$ 67.34
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 1-249	RN-ETP-000249-PPL1Y	$ 74.52	$ 64.83
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 1-249	RN-ETP-000249-PPL2Y	$ 149.04	$ 129.66
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 1-249	RN-ETP-000249-PPL3Y	$ 201.20	$ 175.04
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 1-249	RN-ETP-000249-PPL4Y	$ 268.27	$ 233.39
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-000249-USP1Y	$ 74.52	$ 64.83
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-000249-USP2Y	$ 149.04	$ 129.66
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-000249-USP3Y	$ 201.20	$ 175.04
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-000249-USP4Y	$ 268.27	$ 233.39
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 250-499	RN-ETP-000499-PPL1Y	$ 61.52	$ 53.52
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 250-499	RN-ETP-000499-PPL2Y	$ 123.04	$ 107.04
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 250-499	RN-ETP-000499-PPL3Y	$ 166.10	$ 144.51
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 250-499	RN-ETP-000499-PPL4Y	$ 221.47	$ 192.68
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-000499-USP1Y	$ 61.52	$ 53.52
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-000499-USP2Y	$ 123.04	$ 107.04
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-000499-USP3Y	$ 166.10	$ 144.51
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-000499-USP4Y	$ 221.47	$ 192.68
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 500-749	RN-ETP-000749-PPL1Y	$ 52.77	$ 45.91
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 500-749	RN-ETP-000749-PPL2Y	$ 105.54	$ 91.82
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 500-749	RN-ETP-000749-PPL3Y	$ 142.48	$ 123.96
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 500-749	RN-ETP-000749-PPL4Y	$ 189.97	$ 165.27
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-000749-USP1Y	$ 52.77	$ 45.91
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-000749-USP2Y	$ 105.54	$ 91.82
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-000749-USP3Y	$ 142.48	$ 123.96
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-000749-USP4Y	$ 189.97	$ 165.27
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 750-999	RN-ETP-000999-PPL1Y	$ 44.32	$ 38.56
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 750-999	RN-ETP-000999-PPL2Y	$ 88.64	$ 77.12
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 750-999	RN-ETP-000999-PPL3Y	$ 119.66	$ 104.10
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 750-999	RN-ETP-000999-PPL4Y	$ 159.55	$ 138.81
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-000999-USP1Y	$ 44.32	$ 38.56
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-000999-USP2Y	$ 88.64	$ 77.12
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-000999-USP3Y	$ 119.66	$ 104.10
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-000999-USP4Y	$ 159.55	$ 138.81
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-001999-PPL1Y	$ 40.20	$ 34.97
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-001999-PPL2Y	$ 80.40	$ 69.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-001999-PPL3Y	$ 108.54	$ 94.43
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-001999-PPL4Y	$ 144.72	$ 125.91
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-001999-USP1Y	$ 40.20	$ 34.97
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-001999-USP2Y	$ 80.40	$ 69.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-001999-USP3Y	$ 108.54	$ 94.43
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-001999-USP4Y	$ 144.72	$ 125.91
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-004999-PPL1Y	$ 36.59	$ 31.83

FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-004999-PPL2Y	$ 73.18	$ 63.67
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-004999-PPL3Y	$ 98.79	$ 85.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-004999-PPL4Y	$ 131.72	$ 114.60
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-004999-USP1Y	$ 36.59	$ 31.83
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-004999-USP2Y	$ 73.18	$ 63.67
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-004999-USP3Y	$ 98.79	$ 85.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-004999-USP4Y	$ 131.72	$ 114.60
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-009999-PPL1Y	$ 32.59	$ 28.35
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-009999-PPL2Y	$ 65.18	$ 56.71
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-009999-PPL3Y	$ 87.99	$ 76.55
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-009999-PPL4Y	$ 117.32	$ 102.07
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-009999-USP1Y	$ 32.59	$ 28.35
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-009999-USP2Y	$ 65.18	$ 56.71
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-009999-USP3Y	$ 87.99	$ 76.55
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-009999-USP4Y	$ 117.32	$ 102.07
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-019999-PPL1Y	$ 28.13	$ 24.47
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-019999-PPL2Y	$ 56.26	$ 48.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-019999-PPL3Y	$ 75.95	$ 66.08
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-019999-PPL4Y	$ 101.27	$ 88.10
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-019999-USP1Y	$ 28.13	$ 24.47
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-019999-USP2Y	$ 56.26	$ 48.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-019999-USP3Y	$ 75.95	$ 66.08
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-019999-USP4Y	$ 101.27	$ 88.10
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-049999-PPL1Y	$ 26.53	$ 23.08
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-049999-PPL2Y	$ 53.06	$ 46.16
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-049999-PPL3Y	$ 71.63	$ 62.32
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-049999-PPL4Y	$ 95.51	$ 83.09
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-049999-USP1Y	$ 26.53	$ 23.08
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-049999-USP2Y	$ 53.06	$ 46.16
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-049999-USP3Y	$ 71.63	$ 62.32
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-049999-USP4Y	$ 95.51	$ 83.09
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-074999-PPL1Y	$ 23.96	$ 20.85
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-074999-PPL2Y	$ 47.92	$ 41.69
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-074999-PPL3Y	$ 64.69	$ 56.28
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-074999-PPL4Y	$ 86.26	$ 75.05
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-074999-USP1Y	$ 23.96	$ 20.85
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-074999-USP2Y	$ 47.92	$ 41.69
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-074999-USP3Y	$ 64.69	$ 56.28
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-074999-USP4Y	$ 86.26	$ 75.05
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-099999-PPL1Y	$ 20.72	$ 18.03
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-099999-PPL2Y	$ 41.44	$ 36.05
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-099999-PPL3Y	$ 55.94	$ 48.67
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-099999-PPL4Y	$ 74.59	$ 64.89
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-099999-USP1Y	$ 20.72	$ 18.03
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-099999-USP2Y	$ 41.44	$ 36.05
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-099999-USP3Y	$ 55.94	$ 48.67
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-099999-USP4Y	$ 74.59	$ 64.89
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-199999-PPL1Y	$ 18.22	$ 15.85
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-199999-PPL2Y	$ 36.44	$ 31.70

FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-199999-PPL3Y	$ 49.19	$ 42.80
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-199999-PPL4Y	$ 65.59	$ 57.06
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-199999-USP1Y	$ 18.22	$ 15.85
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-199999-USP2Y	$ 36.44	$ 31.70
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-199999-USP3Y	$ 49.19	$ 42.80
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-199999-USP4Y	$ 65.59	$ 57.06
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 200,000+	RN-ETP-200000+PPL1Y	$ 17.20	$ 14.96
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 200,000+	RN-ETP-200000+PPL2Y	$ 34.40	$ 29.93
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 200,000+	RN-ETP-200000+PPL3Y	$ 46.44	$ 40.40
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 200,000+	RN-ETP-200000+PPL4Y	$ 61.92	$ 53.87
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-200000+USP1Y	$ 17.20	$ 14.96
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-200000+USP2Y	$ 34.40	$ 29.93
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-200000+USP3Y	$ 46.44	$ 40.40
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-200000+USP4Y	$ 61.92	$ 53.87
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 1-249	RN-ETP-000249-PTM2Y	$ 116.64	$ 101.48
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 1-249	RN-ETP-000249-USG2Y	$ 116.64	$ 101.48
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 250-499	RN-ETP-000499-PTM2Y	$ 96.30	$ 83.78
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 250-499	RN-ETP-000499-USG2Y	$ 96.30	$ 83.78
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 500-749	RN-ETP-000749-PTM2Y	$ 82.60	$ 71.86
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 500-749	RN-ETP-000749-USG2Y	$ 82.60	$ 71.86
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 750-999	RN-ETP-000999-PTM2Y	$ 69.38	$ 60.36
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 750-999	RN-ETP-000999-USG2Y	$ 69.38	$ 60.36
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 1,000-1999	RN-ETP-001999-PTM2Y	$ 62.92	$ 54.74
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 1,000-1999	RN-ETP-001999-USG2Y	$ 62.92	$ 54.74
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 2,000-4999	RN-ETP-004999-PTM2Y	$ 57.28	$ 49.83
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 2,000-4999	RN-ETP-004999-USG2Y	$ 57.28	$ 49.83
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 5,000-9999	RN-ETP-009999-PTM2Y	$ 51.02	$ 44.39
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 5,000-9999	RN-ETP-009999-USG2Y	$ 51.02	$ 44.39
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 10,000-19999	RN-ETP-019999-PTM2Y	$ 44.04	$ 38.31
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 10,000-19999	RN-ETP-019999-USG2Y	$ 44.04	$ 38.31
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 20,000-49999	RN-ETP-049999-PTM2Y	$ 41.52	$ 36.12
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 20,000-49999	RN-ETP-049999-USG2Y	$ 41.52	$ 36.12
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 50,000-74999	RN-ETP-074999-PTM2Y	$ 37.50	$ 32.63
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 50,000-74999	RN-ETP-074999-USG2Y	$ 37.50	$ 32.63
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 75,000-99999	RN-ETP-099999-PTM2Y	$ 32.44	$ 28.22
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 75,000-99999	RN-ETP-099999-USG2Y	$ 32.44	$ 28.22
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 100,000-199999	RN-ETP-199999-PTM2Y	$ 28.52	$ 24.81
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 100,000-199999	RN-ETP-199999-USG2Y	$ 28.52	$ 24.81
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 200,000+	RN-ETP-200000+PTM2Y	$ 26.92	$ 23.42
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 200,000+	RN-ETP-200000+USG2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Platinum Support 1 Year	ETP-C-PROMO-PTM1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Plat Prio Plus Support 1 Year	ETP-C-PROMO-PPL1Y	$ 26.06	$ 22.67
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov CA 1 Year	ETP-C-PROMO-CAG1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov CA Plat Prio Plus 1 Year	ETP-C-PROMO-CAP1Y	$ 26.06	$ 22.67
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov US 1 Year	ETP-C-PROMO-USG1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov US Plat Prio Plus 1 Year	ETP-C-PROMO-USP1Y	$ 26.06	$ 22.67
FireEye	Professional services custom SKU	PS-OS-CUST	Call for quote	#VALUE!
FireEye	Onsite professional services - includes FTE for 5 days a week for 6 months of services - No travel included - if travel is required please include travel SKU.	PS-OS-LTSER	$ 192,000.00	$ 174,720.00
FireEye	Onsite professional services - includes 40 hrs of services, 4 hrs of proj mgmt AND travel expenses within country. Any travel out of country will require th	PS-OS-T	$ 15,040.00	$ 13,686.40

FireEye	Professional services travel SKU	PS-OS-TRAVEL	$ 500.00	$ 455.00
FireEye	Online Web Training-FireEye Product Overview	EDU-OWT-BSC-OV	$ -	$ -
FireEye	Managed Defense Continuous Vigilance 1 Year 1-249	MDCV-002491Y	$ 1,296.00	$ 1,127.52
FireEye	Managed Defense Continuous Vigilance 2 Year 1-249	MDCV-002492Y	$ 2,592.00	$ 2,255.04
FireEye	Managed Defense Continuous Vigilance 3 Year 1-249	MDCV-002493Y	$ 3,888.00	$ 3,382.56
FireEye	Managed Defense Continuous Vigilance 4 Year 1-249	MDCV-002494Y	$ 5,184.00	$ 4,510.08
FireEye	Managed Defense Continuous Vigilance 5 Year 1-249	MDCV-002495Y	$ 6,480.00	$ 5,637.60
FireEye	Managed Defense Continuous Vigilance 1 Year 250-499	MDCV-004991Y	$ 656.54	$ 571.19
FireEye	Managed Defense Continuous Vigilance 2 Year 250-499	MDCV-004992Y	$ 1,313.08	$ 1,142.38
FireEye	Threat Analytics Platform-Basic Jumpstart-5 Days	PS-TAP-JS-B	$ 35,000.00	$ 30,450.00
FireEye	EVL Threat Analytics Platform Adv Intel Platinum	EVL-TAP	$ -	$ -
FireEye	Managed Defense Continuous Vigilance 3 Year 250-499	MDCV-004993Y	$ 1,969.62	$ 1,713.57
FireEye	Managed Defense Continuous Vigilance 4 Year 250-499	MDCV-004994Y	$ 2,626.16	$ 2,284.76
FireEye	Managed Defense Continuous Vigilance 5 Year 250-499	MDCV-004995Y	$ 3,282.70	$ 2,855.95
FireEye	Managed Defense Continuous Vigilance 1 Year 500-999	MDCV-009991Y	$ 334.80	$ 291.28
FireEye	Managed Defense Continuous Vigilance 2 Year 500-999	MDCV-009992Y	$ 669.60	$ 582.55
FireEye	Managed Defense Continuous Vigilance 3 Year 500-999	MDCV-009993Y	$ 1,004.40	$ 873.83
FireEye	Managed Defense Continuous Vigilance 4 Year 500-999	MDCV-009994Y	$ 1,339.20	$ 1,165.10
FireEye	Managed Defense Continuous Vigilance 5 Year 500-999	MDCV-009995Y	$ 1,674.00	$ 1,456.38
FireEye	Managed Defense Continuous Vigilance 1 Year 1000-1999	MDCV-019991Y	$ 179.28	$ 155.97
FireEye	Managed Defense Continuous Vigilance 2 Year 1000-1999	MDCV-019992Y	$ 358.56	$ 311.95
FireEye	Managed Defense Continuous Vigilance 3 Year 1000-1999	MDCV-019993Y	$ 537.84	$ 467.92
FireEye	Managed Defense Continuous Vigilance 4 Year 1000-1999	MDCV-019994Y	$ 717.12	$ 623.89
FireEye	Managed Defense Continuous Vigilance 5 Year 1000-1999	MDCV-019995Y	$ 896.40	$ 779.87
FireEye	Managed Defense Continuous Vigilance 1 Year 2000-4999	MDCV-049991Y	$ 79.49	$ 69.16
FireEye	Managed Defense Continuous Vigilance 2 Year 2000-4999	MDCV-049992Y	$ 158.98	$ 138.31
FireEye	Managed Defense Continuous Vigilance 3 Year 2000-4999	MDCV-049993Y	$ 238.47	$ 207.47
FireEye	Managed Defense Continuous Vigilance 4 Year 2000-4999	MDCV-049994Y	$ 317.96	$ 276.63
FireEye	Managed Defense Continuous Vigilance 5 Year 2000-4999	MDCV-049995Y	$ 397.45	$ 345.78
FireEye	Managed Defense Continuous Vigilance 1 Year 5000-9999	MDCV-099991Y	$ 62.64	$ 54.50
FireEye	Managed Defense Continuous Vigilance 2 Year 5000-9999	MDCV-099992Y	$ 125.28	$ 108.99
FireEye	Managed Defense Continuous Vigilance 3 Year 5000-9999	MDCV-099993Y	$ 187.92	$ 163.49
FireEye	Managed Defense Continuous Vigilance 4 Year 5000-9999	MDCV-099994Y	$ 250.56	$ 217.99
FireEye	Managed Defense Continuous Vigilance 5 Year 5000-9999	MDCV-099995Y	$ 313.20	$ 272.48
FireEye	Managed Defense Continuous Vigilance 1 Year 100K-149999	MDCV-1499991Y	$ 23.04	$ 20.04
FireEye	Managed Defense Continuous Vigilance 2 Year 100K-149999	MDCV-1499992Y	$ 46.08	$ 40.09
FireEye	Managed Defense Continuous Vigilance 3 Year 100K-149999	MDCV-1499993Y	$ 69.12	$ 60.13
FireEye	Managed Defense Continuous Vigilance 4 Year 100K-149999	MDCV-1499994Y	$ 92.16	$ 80.18
FireEye	Managed Defense Continuous Vigilance 5 Year 100K-149999	MDCV-1499995Y	$ 115.20	$ 100.22
FireEye	Managed Defense Continuous Vigilance 1 Year 10000-19999	MDCV-199991Y	$ 47.41	$ 41.25
FireEye	Managed Defense Continuous Vigilance 2 Year 10000-19999	MDCV-199992Y	$ 94.82	$ 82.49
FireEye	Managed Defense Continuous Vigilance 3 Year 10000-19999	MDCV-199993Y	$ 142.23	$ 123.74
FireEye	Managed Defense Continuous Vigilance 4 Year 10000-19999	MDCV-199994Y	$ 189.64	$ 164.99
FireEye	Managed Defense Continuous Vigilance 5 Year 10000-19999	MDCV-199995Y	$ 237.05	$ 206.23
FireEye	Managed Defense Continuous Vigilance 1 Year 150,000-199,999	MDCV-1999991Y	$ 18.60	$ 16.18
FireEye	Managed Defense Continuous Vigilance 2 Year 150,000-199,999	MDCV-1999992Y	$ 37.20	$ 32.36
FireEye	Managed Defense Continuous Vigilance 3 Year 150,000-199,999	MDCV-1999993Y	$ 55.80	$ 48.55
FireEye	Managed Defense Continuous Vigilance 4 Year 150,000-199,999	MDCV-1999994Y	$ 74.40	$ 64.73
FireEye	Managed Defense Continuous Vigilance 5 Year 150,000-199,999	MDCV-1999995Y	$ 93.00	$ 80.91

FireEye	Managed Defense Continuous Vigilance 1 Year 200,000+	MDCV-200000+1Y	$ 15.40	$ 13.40
FireEye	Managed Defense Continuous Vigilance 2 Year 200,000+	MDCV-200000+2Y	$ 30.80	$ 26.80
FireEye	Managed Defense Continuous Vigilance 3 Year 200,000+	MDCV-200000+3Y	$ 46.20	$ 40.19
FireEye	Managed Defense Continuous Vigilance 4 Year 200,000+	MDCV-200000+4Y	$ 61.60	$ 53.59
FireEye	Managed Defense Continuous Vigilance 5 Year 200,000+	MDCV-200000+5Y	$ 77.00	$ 66.99
FireEye	Managed Defense Continuous Vigilance 1 Year 20000-39999	MDCV-399991Y	$ 41.00	$ 35.67
FireEye	Managed Defense Continuous Vigilance 2 Year 20000-39999	MDCV-399992Y	$ 82.00	$ 71.34
FireEye	Managed Defense Continuous Vigilance 3 Year 20000-39999	MDCV-399993Y	$ 123.00	$ 107.01
FireEye	Managed Defense Continuous Vigilance 4 Year 20000-39999	MDCV-399994Y	$ 164.00	$ 142.68
FireEye	Managed Defense Continuous Vigilance 5 Year 20000-39999	MDCV-399995Y	$ 205.00	$ 178.35
FireEye	Managed Defense Continuous Vigilance 1 Year 40000-59999	MDCV-599991Y	$ 36.00	$ 31.32
FireEye	Managed Defense Continuous Vigilance 2 Year 40000-59999	MDCV-599992Y	$ 72.00	$ 62.64
FireEye	Managed Defense Continuous Vigilance 3 Year 40000-59999	MDCV-599993Y	$ 108.00	$ 93.96
FireEye	Managed Defense Continuous Vigilance 4 Year 40000-59999	MDCV-599994Y	$ 144.00	$ 125.28
FireEye	Managed Defense Continuous Vigilance 5 Year 40000-59999	MDCV-599995Y	$ 180.00	$ 156.60
FireEye	Managed Defense Continuous Vigilance 1 Year 60000-79999	MDCV-799991Y	$ 30.00	$ 26.10
FireEye	Managed Defense Continuous Vigilance 2 Year 60000-79999	MDCV-799992Y	$ 60.00	$ 52.20
FireEye	Managed Defense Continuous Vigilance 3 Year 60000-79999	MDCV-799993Y	$ 90.00	$ 78.30
FireEye	Managed Defense Continuous Vigilance 4 Year 60000-79999	MDCV-799994Y	$ 120.00	$ 104.40
FireEye	Managed Defense Continuous Vigilance 5 Year 60000-79999	MDCV-799995Y	$ 150.00	$ 130.50
FireEye	Managed Defense Continuous Vigilance 1 Year 80000-99999	MDCV-999991Y	$ 26.72	$ 23.25
FireEye	Managed Defense Continuous Vigilance 2 Year 80000-99999	MDCV-999992Y	$ 53.44	$ 46.49
FireEye	Managed Defense Continuous Vigilance 3 Year 80000-99999	MDCV-999993Y	$ 80.16	$ 69.74
FireEye	Managed Defense Continuous Vigilance 4 Year 80000-99999	MDCV-999994Y	$ 106.88	$ 92.99
FireEye	Managed Defense Continuous Vigilance 5 Year 80000-99999	MDCV-999995Y	$ 133.60	$ 116.23
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 1-249	RN-MDCV-002491Y	$ 1,296.00	$ 1,127.52
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 1-249	RN-MDCV-002492Y	$ 2,592.00	$ 2,255.04
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 1-249	RN-MDCV-002493Y	$ 3,888.00	$ 3,382.56
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 1-249	RN-MDCV-002494Y	$ 5,184.00	$ 4,510.08
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 250-499	RN-MDCV-004991Y	$ 656.64	$ 571.28
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 250-499	RN-MDCV-004992Y	$ 1,313.28	$ 1,142.55
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 250-499	RN-MDCV-004993Y	$ 1,969.92	$ 1,713.83
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 250-499	RN-MDCV-004994Y	$ 2,626.56	$ 2,285.11
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 500-999	RN-MDCV-009991Y	$ 334.80	$ 291.28
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 500-999	RN-MDCV-009992Y	$ 669.60	$ 582.55
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 500-999	RN-MDCV-009993Y	$ 1,004.40	$ 873.83
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 500-999	RN-MDCV-009994Y	$ 1,339.20	$ 1,165.10
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 1000-1999	RN-MDCV-019991Y	$ 179.28	$ 155.97
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 1000-1999	RN-MDCV-019992Y	$ 358.56	$ 311.95
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 1000-1999	RN-MDCV-019993Y	$ 537.84	$ 467.92
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 1000-1999	RN-MDCV-019994Y	$ 717.12	$ 623.89
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 2000-4999	RN-MDCV-049991Y	$ 79.49	$ 69.16
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 2000-4999	RN-MDCV-049992Y	$ 158.98	$ 138.31
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 2000-4999	RN-MDCV-049993Y	$ 238.47	$ 207.47
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 2000-4999	RN-MDCV-049994Y	$ 317.96	$ 276.63
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 5000-9999	RN-MDCV-099991Y	$ 62.64	$ 54.50
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 5000-9999	RN-MDCV-099992Y	$ 125.28	$ 108.99
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 5000-9999	RN-MDCV-099993Y	$ 187.92	$ 163.49
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 5000-9999	RN-MDCV-099994Y	$ 250.56	$ 217.99

FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 100K-149999	RN-MDCV-1499991Y	$ 23.04	$ 20.04
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 100K-149999	RN-MDCV-1499992Y	$ 46.08	$ 40.09
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 100K-149999	RN-MDCV-1499993Y	$ 69.12	$ 60.13
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 100K-149999	RN-MDCV-1499994Y	$ 92.16	$ 80.18
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 10000-19999	RN-MDCV-199991Y	$ 47.41	$ 41.25
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 10000-19999	RN-MDCV-199992Y	$ 94.82	$ 82.49
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 10000-19999	RN-MDCV-199993Y	$ 142.23	$ 123.74
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 10000-19999	RN-MDCV-199994Y	$ 189.64	$ 164.99
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 150,000-199,999	RN-MDCV-1999991Y	$ 18.60	$ 16.18
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 150,000-199,999	RN-MDCV-1999992Y	$ 37.20	$ 32.36
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 150,000-199,999	RN-MDCV-1999993Y	$ 55.80	$ 48.55
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 150,000-199,999	RN-MDCV-1999994Y	$ 74.40	$ 64.73
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 200,000+	RN-MDCV-200000+1Y	$ 15.40	$ 13.40
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 200,000+	RN-MDCV-200000+2Y	$ 30.80	$ 26.80
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 200,000+	RN-MDCV-200000+3Y	$ 46.20	$ 40.19
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 200,000+	RN-MDCV-200000+4Y	$ 61.60	$ 53.59
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 20000-39999	RN-MDCV-399991Y	$ 41.00	$ 35.67
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 20000-39999	RN-MDCV-399992Y	$ 82.00	$ 71.34
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 20000-39999	RN-MDCV-399993Y	$ 123.00	$ 107.01
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 20000-39999	RN-MDCV-399994Y	$ 164.00	$ 142.68
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 40000-59999	RN-MDCV-599991Y	$ 36.00	$ 31.32
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 40000-59999	RN-MDCV-599992Y	$ 72.00	$ 62.64
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 40000-59999	RN-MDCV-599993Y	$ 108.00	$ 93.96
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 40000-59999	RN-MDCV-599994Y	$ 144.00	$ 125.28
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 60000-79999	RN-MDCV-799991Y	$ 30.00	$ 26.10
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 60000-79999	RN-MDCV-799992Y	$ 60.00	$ 52.20
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 60000-79999	RN-MDCV-799994Y	$ 120.00	$ 104.40
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 80000-99999	RN-MDCV-999991Y	$ 26.72	$ 23.25
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 80000-99999	RN-MDCV-999992Y	$ 53.44	$ 46.49
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 80000-99999	RN-MDCV-999993Y	$ 80.16	$ 69.74
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 80000-99999	RN-MDCV-999994Y	$ 106.88	$ 92.99
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 60000-79999	RN-MDCV-799993Y	$ 90.00	$ 78.30
FireEye	PX 004S Managed Defense Appliance Tech Enabler Bundle	MD-004SPX-TE-BDL	$ 7,000.00	$ 6,090.00
FireEye	PX 2040ESS48 Managed Defense Appliance Tech Enabler	MD-2040ESS48PX-TE-BDL	$ 40,000.00	$ 34,800.00
FireEye	Up to 3 days of services including installation of up to 4 total components (e.g. HX, DMZ, NX, PX) and transition to the FaaS team. Fixed price engageme	CS-FaaS-JS-B	$ 9,000.00	$ 7,830.00
FireEye	Up to 5 days of services including installation of up to 6 total components (e.g. HX, DMZ, NX, PX) and transition to the FaaS team. Fixed price engageme	CS-FaaS-JS-ADV	$ 15,000.00	$ 13,050.00
FireEye	Eval - Mobile Threat Prevention - Application Analysis - 1 Year	EVL-MC-AA	$ -	$ -
FireEye	Eval - Mobile Threat Prevention - API (100 devices) - 1 Year	EVL-MC-MS	$ -	$ -
FireEye	Mobile Threat Prevention - Application Analysis Admin Addon (5 admins) - 1 Year	MC-AA-ADM-1Y	$ 5,000.00	$ 4,350.00
FireEye	Mobile Threat Prevention - Application Analysis Admin Addon (5 admins) - 2 Year	MC-AA-ADM-2Y	$ 10,000.00	$ 8,700.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 1 Year	MC-AA1Y-CAG	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 1 Year	MC-AA1Y-CAP	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 1 Year	MC-AA1Y-PLT	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 1 Year	MC-AA1Y-PPL	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 1 Year	MC-AA1Y-USG	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 1 Year	MC-AA1Y-USP	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 2 Year	MC-AA2Y-CAG	$ 40,000.00	$ 34,800.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 2 Year	MC-AA2Y-CAP	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 2 Year	MC-AA2Y-PLT	$ 40,000.00	$ 34,800.00

FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 2 Year	MC-AA2Y-PPL	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 2 Year	MC-AA2Y-USG	$ 40,000.00	$ 34,800.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 2 Year	MC-AA2Y-USP	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 3 Year	MC-AA3Y-CAG	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 3 Year	MC-AA3Y-CAP	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 3 Year	MC-AA3Y-PLT	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 3 Year	MC-AA3Y-PPL	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 3 Year	MC-AA3Y-USG	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 3 Year	MC-AA3Y-USP	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 4 Year	MC-AA4Y-CAG	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 4 Year	MC-AA4Y-CAP	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 4 Year	MC-AA4Y-PLT	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 4 Year	MC-AA4Y-PPL	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 4 Year	MC-AA4Y-USG	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 4 Year	MC-AA4Y-USP	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 5 Year	MC-AA5Y-CAG	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 5 Year	MC-AA5Y-CAP	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 5 Year	MC-AA5Y-PLT	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 5 Year	MC-AA5Y-PPL	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 5 Year	MC-AA5Y-USG	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 5 Year	MC-AA5Y-USP	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - API 1 Year 100-499	MC-MS-000499-1Y	$ 99.00	$ 86.13
FireEye	Mobile Threat Prevention - API 2 Year 100-499	MC-MS-000499-2Y	$ 198.00	$ 172.26
FireEye	Mobile Threat Prevention - API 3 Year 100-499	MC-MS-000499-3Y	$ 260.00	$ 226.20
FireEye	Mobile Threat Prevention - API 4 Year 100-499	MC-MS-000499-4Y	$ 340.00	$ 295.80
FireEye	Mobile Threat Prevention - API 5 Year 100-499	MC-MS-000499-5Y	$ 430.00	$ 374.10
FireEye	Mobile Threat Prevention - API 1 Year 500-999	MC-MS-000999-1Y	$ 88.00	$ 76.56
FireEye	Mobile Threat Prevention - API 2 Year 500-999	MC-MS-000999-2Y	$ 176.00	$ 153.12
FireEye	Mobile Threat Prevention - API 3 Year 500-999	MC-MS-000999-3Y	$ 230.00	$ 200.10
FireEye	Mobile Threat Prevention - API 4 Year 500-999	MC-MS-000999-4Y	$ 300.00	$ 261.00
FireEye	Mobile Threat Prevention - API 5 Year 500-999	MC-MS-000999-5Y	$ 380.00	$ 330.60
FireEye	Mobile Threat Prevention - API 1 Year 1K-1999	MC-MS-001999-1Y	$ 79.00	$ 68.73
FireEye	Mobile Threat Prevention - API 2 Year 1K-1999	MC-MS-001999-2Y	$ 158.00	$ 137.46
FireEye	Mobile Threat Prevention - API 3 Year 1K-1999	MC-MS-001999-3Y	$ 210.00	$ 182.70
FireEye	Mobile Threat Prevention - API 4 Year 1K-1999	MC-MS-001999-4Y	$ 270.00	$ 234.90
FireEye	Mobile Threat Prevention - API 5 Year 1K-1999	MC-MS-001999-5Y	$ 340.00	$ 295.80
FireEye	Mobile Threat Prevention - API 1 Year 2K-4999	MC-MS-004999-1Y	$ 71.00	$ 61.77
FireEye	Mobile Threat Prevention - API 2 Year 2K-4999	MC-MS-004999-2Y	$ 142.00	$ 123.54
FireEye	Mobile Threat Prevention - API 3 Year 2K-4999	MC-MS-004999-3Y	$ 190.00	$ 165.30
FireEye	Mobile Threat Prevention - API 4 Year 2K-4999	MC-MS-004999-4Y	$ 250.00	$ 217.50
FireEye	Mobile Threat Prevention - API 5 Year 2K-4999	MC-MS-004999-5Y	$ 310.00	$ 269.70
FireEye	Mobile Threat Prevention - API 1 Year 5K-9999	MC-MS-009999-1Y	$ 63.00	$ 54.81
FireEye	Mobile Threat Prevention - API 2 Year 5K-9999	MC-MS-009999-2Y	$ 126.00	$ 109.62
FireEye	Mobile Threat Prevention - API 3 Year 5K-9999	MC-MS-009999-3Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 4 Year 5K-9999	MC-MS-009999-4Y	$ 220.00	$ 191.40
FireEye	Mobile Threat Prevention - API 5 Year 5K-9999	MC-MS-009999-5Y	$ 270.00	$ 234.90
FireEye	Mobile Threat Prevention - API 1 Year 10K-19999	MC-MS-019999-1Y	$ 56.00	$ 48.72
FireEye	Mobile Threat Prevention - API 2 Year 10K-19999	MC-MS-019999-2Y	$ 112.00	$ 97.44
FireEye	Mobile Threat Prevention - API 3 Year 10K-19999	MC-MS-019999-3Y	$ 150.00	$ 130.50

FireEye	Mobile Threat Prevention - API 4 Year 10K-19999	MC-MS-019999-4Y	$ 200.00	$ 174.00
FireEye	Mobile Threat Prevention - API 5 Year 10K-19999	MC-MS-019999-5Y	$ 240.00	$ 208.80
FireEye	Mobile Threat Prevention - API 1 Year 20K-49999	MC-MS-049999-1Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - API 2 Year 20K-49999	MC-MS-049999-2Y	$ 100.00	$ 87.00
FireEye	Mobile Threat Prevention - API 3 Year 20K-49999	MC-MS-049999-3Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - API 4 Year 20K-49999	MC-MS-049999-4Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 5 Year 20K-49999	MC-MS-049999-5Y	$ 220.00	$ 191.40
FireEye	Mobile Threat Prevention - API 1 Year 50K-74999	MC-MS-074999-1Y	$ 45.00	$ 39.15
FireEye	Mobile Threat Prevention - API 2 Year 50K-74999	MC-MS-074999-2Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - API 3 Year 50K-74999	MC-MS-074999-3Y	$ 120.00	$ 104.40
FireEye	Mobile Threat Prevention - API 4 Year 50K-74999	MC-MS-074999-4Y	$ 160.00	$ 139.20
FireEye	Mobile Threat Prevention - API 5 Year 50K-74999	MC-MS-074999-5Y	$ 200.00	$ 174.00
FireEye	Mobile Threat Prevention - API 1 Year 75K-99999	MC-MS-099999-1Y	$ 40.00	$ 34.80
FireEye	Mobile Threat Prevention - API 2 Year 75K-99999	MC-MS-099999-2Y	$ 80.00	$ 69.60
FireEye	Mobile Threat Prevention - API 3 Year 75K-99999	MC-MS-099999-3Y	$ 110.00	$ 95.70
FireEye	Mobile Threat Prevention - API 4 Year 75K-99999	MC-MS-099999-4Y	$ 140.00	$ 121.80
FireEye	Mobile Threat Prevention - API 5 Year 75K-99999	MC-MS-099999-5Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 1 Year 100000+	MC-MS-100000+-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - API 2 Year 100000+	MC-MS-100000+-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - API 3 Year 100000+	MC-MS-100000+-3Y	$ 100.00	$ 87.00
FireEye	Mobile Threat Prevention - API 4 Year 100000+	MC-MS-100000+-4Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - API 5 Year 100000+	MC-MS-100000+-5Y	$ 160.00	$ 139.20
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 1 Year	RN-MC-AA1Y-CAG	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 1 Year	RN-MC-AA1Y-CAP	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 1 Year	RN-MC-AA1Y-PLT	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 1 Year	RN-MC-AA1Y-PPL	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 1 Year	RN-MC-AA1Y-USG	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 1 Year	RN-MC-AA1Y-USP	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 2 Year	RN-MC-AA2Y-CAG	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 2 Year	RN-MC-AA2Y-CAP	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 2 Year	RN-MC-AA2Y-PLT	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 2 Year	RN-MC-AA2Y-PPL	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 2 Year	RN-MC-AA2Y-USG	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 2 Year	RN-MC-AA2Y-USP	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 3 Year	RN-MC-AA3Y-CAG	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 3 Year	RN-MC-AA3Y-CAP	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 3 Year	RN-MC-AA3Y-PLT	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 3 Year	RN-MC-AA3Y-PPL	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 3 Year	RN-MC-AA3Y-USG	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 3 Year	RN-MC-AA3Y-USP	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 4 Year	RN-MC-AA4Y-CAG	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 4 Year	RN-MC-AA4Y-CAP	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 4 Year	RN-MC-AA4Y-PLT	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 4 Year	RN-MC-AA4Y-PPL	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 4 Year	RN-MC-AA4Y-USG	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 4 Year	RN-MC-AA4Y-USP	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 100-499	RN-MC-MS-000499-1Y	$ 99.00	$ 86.13
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 100-499	RN-MC-MS-000499-2Y	$ 260.00	$ 226.20
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 100-499	RN-MC-MS-000499-3Y	$ 340.00	$ 295.80

FireEye	Renewal-Mobile Threat Prevention - API 4 Year 100-499	RN-MC-MS-000499-4Y	$ 430.00	$ 374.10
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 500-999	RN-MC-MS-000999-1Y	$ 88.00	$ 76.56
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 500-999	RN-MC-MS-000999-2Y	$ 230.00	$ 200.10
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 500-999	RN-MC-MS-000999-3Y	$ 300.00	$ 261.00
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 500-999	RN-MC-MS-000999-4Y	$ 380.00	$ 330.60
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 1K-1999	RN-MC-MS-001999-1Y	$ 79.00	$ 68.73
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 1K-1999	RN-MC-MS-001999-2Y	$ 210.00	$ 182.70
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 1K-1999	RN-MC-MS-001999-3Y	$ 270.00	$ 234.90
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 1K-1999	RN-MC-MS-001999-4Y	$ 340.00	$ 295.80
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 2K-4999	RN-MC-MS-004999-1Y	$ 71.00	$ 61.77
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 2K-4999	RN-MC-MS-004999-2Y	$ 190.00	$ 165.30
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 2K-4999	RN-MC-MS-004999-3Y	$ 250.00	$ 217.50
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 2K-4999	RN-MC-MS-004999-4Y	$ 310.00	$ 269.70
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 5K-9999	RN-MC-MS-009999-1Y	$ 63.00	$ 54.81
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 5K-9999	RN-MC-MS-009999-2Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 5K-9999	RN-MC-MS-009999-3Y	$ 220.00	$ 191.40
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 5K-9999	RN-MC-MS-009999-4Y	$ 270.00	$ 234.90
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 10K-19999	RN-MC-MS-019999-1Y	$ 56.00	$ 48.72
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 10K-19999	RN-MC-MS-019999-2Y	$ 150.00	$ 130.50
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 10K-19999	RN-MC-MS-019999-3Y	$ 200.00	$ 174.00
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 10K-19999	RN-MC-MS-019999-4Y	$ 240.00	$ 208.80
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 20K-49999	RN-MC-MS-049999-1Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 20K-49999	RN-MC-MS-049999-2Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 20K-49999	RN-MC-MS-049999-3Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 20K-49999	RN-MC-MS-049999-4Y	$ 220.00	$ 191.40
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 50K-74999	RN-MC-MS-074999-1Y	$ 45.00	$ 39.15
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 50K-74999	RN-MC-MS-074999-2Y	$ 120.00	$ 104.40
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 50K-74999	RN-MC-MS-074999-3Y	$ 160.00	$ 139.20
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 50K-74999	RN-MC-MS-074999-4Y	$ 200.00	$ 174.00
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 75K-99999	RN-MC-MS-099999-1Y	$ 40.00	$ 34.80
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 75K-99999	RN-MC-MS-099999-2Y	$ 110.00	$ 95.70
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 75K-99999	RN-MC-MS-099999-3Y	$ 140.00	$ 121.80
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 75K-99999	RN-MC-MS-099999-4Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 100000+	RN-MC-MS-100000+-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 100000+	RN-MC-MS-100000+-2Y	$ 100.00	$ 87.00
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 100000+	RN-MC-MS-100000+-3Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 100000+	RN-MC-MS-100000+-4Y	$ 160.00	$ 139.20
FireEye	MX 900 Appliance - Mobile Threat Prevention - Mobile Security Management	900MX-HW	$ 7,995.00	$ 6,955.65
FireEye	MX 900 Appliance Standby- Mobile Threat Prevention - Mobile Security Management	900MX-HWSB	$ 7,995.00	$ 6,955.65
FireEye	EVAL-MX 900 appliance - Mobile Threat Prevention - Mobile Security Management	EVL-900MX-HW	$ 1,450.00	$ 1,261.50
FireEye	POC-MX 900 appliance - Mobile Threat Prevention - Mobile Security Management	POC-900MX-HW	$ 1,450.00	$ 1,261.50
FireEye	Eval - Mobile Threat Prevention - Mobile Security Management 1 Year 100 devices	EVL-MC-MSM	$ -	$ -
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 100-499	MC-MSM-000499-1Y	$ 62.00	$ 53.94
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 100-499	MC-MSM-000499-2Y	$ 124.00	$ 107.88
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 100-499	MC-MSM-000499-3Y	$ 159.00	$ 138.33
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 100-499	MC-MSM-000499-4Y	$ 211.00	$ 183.57
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 100-499	MC-MSM-000499-5Y	$ 264.00	$ 229.68
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 500-999	MC-MSM-000999-1Y	$ 52.00	$ 45.24
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 500-999	MC-MSM-000999-2Y	$ 104.00	$ 90.48

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 500-999	RN-MC-MSM-000999-2Y	$ 104.00	$ 90.48
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 500-999	MC-MSM-000999-3Y	$ 133.00	$ 115.71
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 500-999	MC-MSM-000999-4Y	$ 177.00	$ 153.99
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 500-999	MC-MSM-000999-5Y	$ 221.00	$ 192.27
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 1000-1999	MC-MSM-001999-1Y	$ 43.00	$ 37.41
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 1000-1999	MC-MSM-001999-2Y	$ 86.00	$ 74.82
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 1000-1999	MC-MSM-001999-3Y	$ 110.00	$ 95.70
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 1000-1999	MC-MSM-001999-4Y	$ 147.00	$ 127.89
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 1000-1999	MC-MSM-001999-5Y	$ 183.00	$ 159.21
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 2000-4999	MC-MSM-004999-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 2000-4999	MC-MSM-004999-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 2000-4999	MC-MSM-004999-3Y	$ 92.00	$ 80.04
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 2000-4999	MC-MSM-004999-4Y	$ 123.00	$ 107.01
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 2000-4999	MC-MSM-004999-5Y	$ 153.00	$ 133.11
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 5000-9999	MC-MSM-009999-1Y	$ 30.00	$ 26.10
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 5000-9999	MC-MSM-009999-2Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 5000-9999	MC-MSM-009999-3Y	$ 77.00	$ 66.99
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 5000-9999	MC-MSM-009999-4Y	$ 102.00	$ 88.74
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 5000-9999	MC-MSM-009999-5Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 10000-19999	MC-MSM-019999-1Y	$ 25.00	$ 21.75
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 10000-19999	MC-MSM-019999-2Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 10000-19999	MC-MSM-019999-3Y	$ 64.00	$ 55.68
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 10000-19999	MC-MSM-019999-4Y	$ 85.00	$ 73.95
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 10000-19999	MC-MSM-019999-5Y	$ 107.00	$ 93.09
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 20000-49999	MC-MSM-049999-1Y	$ 21.00	$ 18.27
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 20000-49999	MC-MSM-049999-2Y	$ 42.00	$ 36.54
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 20000-49999	MC-MSM-049999-3Y	$ 54.00	$ 46.98
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 20000-49999	MC-MSM-049999-4Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 20000-49999	MC-MSM-049999-5Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 50000-74999	MC-MSM-074999-1Y	$ 17.00	$ 14.79
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 50000-74999	MC-MSM-074999-2Y	$ 34.00	$ 29.58
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 50000-74999	MC-MSM-074999-3Y	$ 44.00	$ 38.28
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 50000-74999	MC-MSM-074999-4Y	$ 58.00	$ 50.46
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 50000-74999	MC-MSM-074999-5Y	$ 73.00	$ 63.51
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 75000-99999	MC-MSM-099999-1Y	$ 14.00	$ 12.18
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 75000-99999	MC-MSM-099999-2Y	$ 28.00	$ 24.36
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 75000-99999	MC-MSM-099999-3Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 75000-99999	MC-MSM-099999-4Y	$ 48.00	$ 41.76
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 75000-99999	MC-MSM-099999-5Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 100000+	MC-MSM-100000+1Y	$ 12.00	$ 10.44
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 100000+	MC-MSM-100000+2Y	$ 24.00	$ 20.88
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 100000+	MC-MSM-100000+3Y	$ 31.00	$ 26.97
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 100000+	MC-MSM-100000+4Y	$ 41.00	$ 35.67
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 100000+	MC-MSM-100000+5Y	$ 51.00	$ 44.37
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 100-499	RN-MC-MSM-000499-1Y	$ 62.00	$ 53.94
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 100-499	RN-MC-MSM-000499-2Y	$ 124.00	$ 107.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 100-499	RN-MC-MSM-000499-3Y	$ 159.00	$ 138.33
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 100-499	RN-MC-MSM-000499-4Y	$ 211.00	$ 183.57
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 100-499	RN-MC-MSM-000499-5Y	$ 264.00	$ 229.68

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 500-999	RN-MC-MSM-000999-1Y	$ 52.00	$ 45.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 500-999	RN-MC-MSM-000999-3Y	$ 133.00	$ 115.71
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 500-999	RN-MC-MSM-000999-4Y	$ 177.00	$ 153.99
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 500-999	RN-MC-MSM-000999-5Y	$ 221.00	$ 192.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 1000-1999	RN-MC-MSM-001999-1Y	$ 43.00	$ 37.41
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 1000-1999	RN-MC-MSM-001999-2Y	$ 86.00	$ 74.82
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 1000-1999	RN-MC-MSM-001999-3Y	$ 110.00	$ 95.70
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 1000-1999	RN-MC-MSM-001999-4Y	$ 147.00	$ 127.89
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 1000-1999	RN-MC-MSM-001999-5Y	$ 183.00	$ 159.21
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 2000-4999	RN-MC-MSM-004999-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 2000-4999	RN-MC-MSM-004999-2Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 2000-4999	RN-MC-MSM-004999-3Y	$ 92.00	$ 80.04
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 2000-4999	RN-MC-MSM-004999-4Y	$ 123.00	$ 107.01
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 2000-4999	RN-MC-MSM-004999-5Y	$ 153.00	$ 133.11
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 5000-9999	RN-MC-MSM-009999-1Y	$ 30.00	$ 26.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 5000-9999	RN-MC-MSM-009999-2Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 5000-9999	RN-MC-MSM-009999-3Y	$ 77.00	$ 66.99
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 5000-9999	RN-MC-MSM-009999-4Y	$ 102.00	$ 88.74
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 5000-9999	RN-MC-MSM-009999-5Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 10000-19999	RN-MC-MSM-019999-1Y	$ 25.00	$ 21.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 10000-19999	RN-MC-MSM-019999-2Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 10000-19999	RN-MC-MSM-019999-3Y	$ 64.00	$ 55.68
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 10000-19999	RN-MC-MSM-019999-4Y	$ 85.00	$ 73.95
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 10000-19999	RN-MC-MSM-019999-5Y	$ 107.00	$ 93.09
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 20000-49999	RN-MC-MSM-049999-1Y	$ 21.00	$ 18.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 20000-49999	RN-MC-MSM-049999-2Y	$ 42.00	$ 36.54
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 20000-49999	RN-MC-MSM-049999-3Y	$ 54.00	$ 46.98
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 20000-49999	RN-MC-MSM-049999-4Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 20000-49999	RN-MC-MSM-049999-5Y	$ 90.00	$ 78.30
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 50000-74999	RN-MC-MSM-074999-1Y	$ 17.00	$ 14.79
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 50000-74999	RN-MC-MSM-074999-2Y	$ 34.00	$ 29.58
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 50000-74999	RN-MC-MSM-074999-3Y	$ 44.00	$ 38.28
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 50000-74999	RN-MC-MSM-074999-4Y	$ 58.00	$ 50.46
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 50000-74999	RN-MC-MSM-074999-5Y	$ 73.00	$ 63.51
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 75000-99999	RN-MC-MSM-099999-1Y	$ 14.00	$ 12.18
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 75000-99999	RN-MC-MSM-099999-2Y	$ 28.00	$ 24.36
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 75000-99999	RN-MC-MSM-099999-3Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 75000-99999	RN-MC-MSM-099999-4Y	$ 48.00	$ 41.76
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 75000-99999	RN-MC-MSM-099999-5Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 100000+	RN-MC-MSM-100000+1Y	$ 12.00	$ 10.44
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 100000+	RN-MC-MSM-100000+2Y	$ 24.00	$ 20.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 100000+	RN-MC-MSM-100000+3Y	$ 31.00	$ 26.97
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 100000+	RN-MC-MSM-100000+4Y	$ 41.00	$ 35.67
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 100000+	RN-MC-MSM-100000+5Y	$ 51.00	$ 44.37
FireEye	MX 900 Support Government CA 1 Year	900MX-CAG1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Government CA 2 Year	900MX-CAG2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Government CA 3 Year	900MX-CAG3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Government CA 4 Year	900MX-CAG4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Government CA 5 Year	900MX-CAG5Y	$ 6,400.00	$ 5,568.00

FireEye	MX 900 Support Government CA Priorioty Plus 1 Year	900MX-CAP1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Government CA Priorioty Plus 2 Year	900MX-CAP2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Government CA Priorioty Plus 3 Year	900MX-CAP3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Government CA Priorioty Plus 4 Year	900MX-CAP4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government CA Priorioty Plus 5 Year	900MX-CAP5Y	$ 8,000.00	$ 6,960.00
FireEye	MX 900 Support Platinum Priority Plus 1 Year	900MX-PPL1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Platinum Priority Plus 2 Year	900MX-PPL2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Platinum Priority Plus 3 Year	900MX-PPL3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Platinum Priority Plus 4 Year	900MX-PPL4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Platinum Priority Plus 5 Year	900MX-PPL5Y	$ 8,000.00	$ 6,960.00
FireEye	MX 900 Support Platinum 1 Year	900MX-PTM1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Platinum 2 Year	900MX-PTM2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Platinum 3 Year	900MX-PTM3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Platinum 4 Year	900MX-PTM4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Platinum 5 Year	900MX-PTM5Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US 1 Year	900MX-USG1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Government US 2 Year	900MX-USG2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Government US 3 Year	900MX-USG3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Government US 4 Year	900MX-USG4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Government US 5 Year	900MX-USG5Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US Priorioty Plus 1 Year	900MX-USP1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Government US Priorioty Plus 2 Year	900MX-USP2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Government US Priorioty Plus 3 Year	900MX-USP3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Government US Priorioty Plus 4 Year	900MX-USP4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US Priorioty Plus 5 Year	900MX-USP5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Government CA 1 Year	RN-900MX-CAG1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Government CA 2 Year	RN-900MX-CAG2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Government CA 3 Year	RN-900MX-CAG3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Government CA 4 Year	RN-900MX-CAG4Y	$ 5,120.00	$ 4,454.40
FireEye	Renewal MX 900 Support Government CA 5 Year	RN-900MX-CAG5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 1 Year	RN-900MX-CAP1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal-MX 900 Support Government CA Priorioty Plus 2 Year	RN-900MX-CAP2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 3 Year	RN-900MX-CAP3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 4 Year	RN-900MX-CAP4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 5 Year	RN-900MX-CAP5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 1 Year	RN-900MX-PPL1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 2 Year	RN-900MX-PPL2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 3 Year	RN-900MX-PPL3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 4 Year	RN-900MX-PPL4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 5 Year	RN-900MX-PPL5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Platinum 1 Year	RN-900MX-PTM1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Platinum 2 Year	RN-900MX-PTM2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Platinum 3 Year	RN-900MX-PTM3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Platinum 4 Year	RN-900MX-PTM4Y	$ 5,120.00	$ 4,454.40
FireEye	Renewal MX 900 Support Platinum 5 Year	RN-900MX-PTM5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US 1 Year	RN-900MX-USG1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Government US 2 Year	RN-900MX-USG2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Government US 3 Year	RN-900MX-USG3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Government US 4 Year	RN-900MX-USG4Y	$ 5,120.00	$ 4,454.40

FireEye	Renewal MX 900 Support Government US 5 Year	RN-900MX-USG5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 1 Year	RN-900MX-USP1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal-MX 900 Support Government US Priorioty Plus 2 Year	RN-900MX-USP2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 3 Year	RN-900MX-USP3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 4 Year	RN-900MX-USP4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 5 Year	RN-900MX-USP5Y	$ 8,000.00	$ 6,960.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 1 Year	UP-900MX-GAG2PP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 2 Year	UP-900MX-GAG2PP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 3 Year	UP-900MX-GAG2PP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 4 Year	UP-900MX-GAG2PP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 5 Year	UP-900MX-GAG2PP5Y	$ 1,600.00	$ 1,392.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 1 Year	UP-900MX-PTM2PPP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 2 Year	UP-900MX-PTM2PPP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 3 Year	UP-900MX-PTM2PPP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 4 Year	UP-900MX-PTM2PPP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 5 Year	UP-900MX-PTM2PPP5Y	$ 1,600.00	$ 1,392.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus1 Year	UP-900MX-USG2PP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus2 Year	UP-900MX-USG2PP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus3 Year	UP-900MX-USG2PP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus4 Year	UP-900MX-USG2PP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus5 Year	UP-900MX-USG2PP5Y	$ 1,600.00	$ 1,392.00
FireEye	MX 8400 Appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HW	$ 64,995.00	$ 56,545.65
FireEye	MX 8400 Appliance/Server Standby- Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HWSB	$ 64,995.00	$ 56,545.65
FireEye	EVAL-MX 8400 appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	EVL-8400MX-HW	$ 13,000.00	$ 11,310.00
FireEye	POC-MX 8400 appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	POC-8400MX-HW	$ 13,000.00	$ 11,310.00
FireEye	MX 8400 Support Government CA 1 Year	8400MX-CAG1Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Government CA 2 Year	8400MX-CAG2Y	$ 32,760.00	$ 28,501.20
FireEye	MX 8400 Support Government CA 3 Year	8400MX-CAG3Y	$ 39,312.00	$ 34,201.44
FireEye	MX 8400 Support Government CA 4 Year	8400MX-CAG4Y	$ 52,416.00	$ 45,601.92
FireEye	MX 8400 Support Government CA 5 Year	8400MX-CAG5Y	$ 46,800.00	$ 40,716.00
FireEye	MX 8400 Support Government CA Priorioty Plus 1 Year	8400MX-CAP1Y	$ 19,434.00	$ 16,907.58
FireEye	MX 8400 Support Government CA Priorioty Plus 2 Year	8400MX-CAP2Y	$ 41,858.00	$ 36,416.46
FireEye	MX 8400 Support Government CA Priorioty Plus 3 Year	8400MX-CAP3Y	$ 46,642.00	$ 40,578.54
FireEye	MX 8400 Support Government CA Priorioty Plus 4 Year	8400MX-CAP4Y	$ 95,674.00	$ 83,236.38
FireEye	MX 8400 Support Government CA Priorioty Plus 5 Year	8400MX-CAP5Y	$ 119,592.00	$ 104,045.04
FireEye	MX 8400 Support Platinum Priority Plus 1 Year	8400MX-PPL1Y	$ 14,949.00	$ 13,005.63
FireEye	MX 8400 Support Platinum Priority Plus 2 Year	8400MX-PPL2Y	$ 29,898.00	$ 26,011.26
FireEye	MX 8400 Support Platinum Priority Plus 3 Year	8400MX-PPL3Y	$ 35,878.00	$ 31,213.86
FireEye	MX 8400 Support Platinum Priority Plus 4 Year	8400MX-PPL4Y	$ 47,837.00	$ 41,618.19
FireEye	MX 8400 Support Platinum Priority Plus 5 Year	8400MX-PPL5Y	$ 59,796.00	$ 52,022.52
FireEye	MX 8400 Support Platinum 1 Year	8400MX-PTM1Y	$ 11,700.00	$ 10,179.00
FireEye	MX 8400 Support Platinum 2 Year	8400MX-PTM2Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Platinum 3 Year	8400MX-PTM3Y	$ 28,080.00	$ 24,429.60
FireEye	MX 8400 Support Platinum 4 Year	8400MX-PTM4Y	$ 37,440.00	$ 32,572.80
FireEye	MX 8400 Support Platinum 5 Year	8400MX-PTM5Y	$ 46,800.00	$ 40,716.00
FireEye	MX 8400 Support Government US 1 Year	8400MX-USG1Y	$ 15,210.00	$ 13,232.70
FireEye	MX 8400 Support Government US 2 Year	8400MX-USG2Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Government US 3 Year	8400MX-USG3Y	$ 36,504.00	$ 31,758.48
FireEye	MX 8400 Support Government US 4 Year	8400MX-USG4Y	$ 48,672.00	$ 42,344.64

FireEye	MX 8400 Support Government US 5 Year	8400MX-USG5Y	$ 60,840.00	$ 52,930.80
FireEye	MX 8400 Support Government US Priorioty Plus 1 Year	8400MX-USP1Y	$ 20,929.00	$ 18,208.23
FireEye	MX 8400 Support Government US Priorioty Plus 2 Year	8400MX-USP2Y	$ 38,868.00	$ 33,815.16
FireEye	MX 8400 Support Government US Priorioty Plus 3 Year	8400MX-USP3Y	$ 46,642.00	$ 40,578.54
FireEye	MX 8400 Support Government US Priorioty Plus 4 Year	8400MX-USP4Y	$ 47,837.00	$ 41,618.19
FireEye	MX 8400 Support Government US Priorioty Plus 5 Year	8400MX-USP5Y	$ 83,715.00	$ 72,832.05
FireEye	Renewal MX 8400 Support Government CA 1 Year	RN-8400MX-CAG1Y	$ 15,210.00	$ 13,232.70
FireEye	Renewal MX 8400 Support Government CA 2 Year	RN-8400MX-CAG2Y	$ 23,400.00	$ 20,358.00
FireEye	Renewal MX 8400 Support Government CA 3 Year	RN-8400MX-CAG3Y	$ 28,080.00	$ 24,429.60
FireEye	Renewal MX 8400 Support Government CA 4 Year	RN-8400MX-CAG4Y	$ 74,880.00	$ 65,145.60
FireEye	Renewal MX 8400 Support Government CA 5 Year	RN-8400MX-CAG5Y	$ 93,600.00	$ 81,432.00
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 1 Year	RN-8400MX-CAP1Y	$ 19,434.00	$ 16,907.58
FireEye	Renewal-MX 8400 Support Government CA Priorioty Plus 2 Year	RN-8400MX-CAP2Y	$ 29,898.00	$ 26,011.26
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 3 Year	RN-8400MX-CAP3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 4 Year	RN-8400MX-CAP4Y	$ 62,189.00	$ 54,104.43
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 5 Year	RN-8400MX-CAP5Y	$ 77,735.00	$ 67,629.45
FireEye	Renewal MX 8400 Support Platinum Priority Plus 1 Year	RN-8400MX-PPL1Y	$ 14,949.00	$ 13,005.63
FireEye	Renewal MX 8400 Support Platinum Priority Plus 2 Year	RN-8400MX-PPL2Y	$ 29,898.00	$ 26,011.26
FireEye	Renewal MX 8400 Support Platinum Priority Plus 3 Year	RN-8400MX-PPL3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Platinum Priority Plus 4 Year	RN-8400MX-PPL4Y	$ 47,837.00	$ 41,618.19
FireEye	Renewal MX 8400 Support Platinum Priority Plus 5 Year	RN-8400MX-PPL5Y	$ 59,796.00	$ 52,022.52
FireEye	Renewal MX 8400 Support Platinum 1 Year	RN-8400MX-PTM1Y	$ 11,700.00	$ 10,179.00
FireEye	Renewal MX 8400 Support Platinum 2 Year	RN-8400MX-PTM2Y	$ 23,400.00	$ 20,358.00
FireEye	Renewal MX 8400 Support Platinum 3 Year	RN-8400MX-PTM3Y	$ 28,080.00	$ 24,429.60
FireEye	Renewal MX 8400 Support Platinum 4 Year	RN-8400MX-PTM4Y	$ 37,440.00	$ 32,572.80
FireEye	Renewal MX 8400 Support Platinum 5 Year	RN-8400MX-PTM5Y	$ 46,800.00	$ 40,716.00
FireEye	Renewal MX 8400 Support Government US 1 Year	RN-8400MX-USG1Y	$ 11,700.00	$ 10,179.00
FireEye	Renewal MX 8400 Support Government US 2 Year	RN-8400MX-USG2Y	$ 30,420.00	$ 26,465.40
FireEye	Renewal MX 8400 Support Government US 3 Year	RN-8400MX-USG3Y	$ 36,504.00	$ 31,758.48
FireEye	Renewal MX 8400 Support Government US 4 Year	RN-8400MX-USG4Y	$ 74,880.00	$ 65,145.60
FireEye	Renewal MX 8400 Support Government US 5 Year	RN-8400MX-USG5Y	$ 93,600.00	$ 81,432.00
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 1 Year	RN-8400MX-USP1Y	$ 19,434.00	$ 16,907.58
FireEye	Renewal-MX 8400 Support Government US Priorioty Plus 2 Year	RN-8400MX-USP2Y	$ 38,868.00	$ 33,815.16
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 3 Year	RN-8400MX-USP3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 4 Year	RN-8400MX-USP4Y	$ 62,189.00	$ 54,104.43
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 5 Year	RN-8400MX-USP5Y	$ 83,715.00	$ 72,832.05
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 1 Year	UP-8400MX-GAG2PP1Y	$ 4,549.00	$ 3,957.63
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 2 Year	UP-8400MX-GAG2PP2Y	$ 8,448.00	$ 7,349.76
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 3 Year	UP-8400MX-GAG2PP3Y	$ 15,596.00	$ 13,568.52
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 4 Year	UP-8400MX-GAG2PP4Y	$ 20,794.00	$ 18,090.78
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 5 Year	UP-8400MX-GAG2PP5Y	$ 25,992.00	$ 22,613.04
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 1 Year	UP-8400MX-PTM2PPP1Y	$ 3,249.00	$ 2,826.63
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 2 Year	UP-8400MX-PTM2PPP2Y	$ 6,498.00	$ 5,653.26
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 3 Year	UP-8400MX-PTM2PPP3Y	$ 7,798.00	$ 6,784.26
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 4 Year	UP-8400MX-PTM2PPP4Y	$ 10,397.00	$ 9,045.39
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 5 Year	UP-8400MX-PTM2PPP5Y	$ 12,996.00	$ 11,306.52
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus1 Year	UP-8400MX-USG2PP1Y	$ 3,249.00	$ 2,826.63
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus2 Year	UP-8400MX-USG2PP2Y	$ 8,448.00	$ 7,349.76
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus3 Year	UP-8400MX-USG2PP3Y	$ 7,798.00	$ 6,784.26

FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus4 Year	UP-8400MX-USG2PP4Y	$ 20,794.00	$ 18,090.78
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus5 Year	UP-8400MX-USG2PP5Y	$ 16,895.00	$ 14,698.65
FireEye	Online Web Training-30-day access to eLearning, self-paced, course on Mobile Threat Prevention Cloud Deployment	EDU-OWT-BSC-MTP	$ 295.00	$ 256.65
FireEye	Eval - Mobile Threat Prevention - Mobile Security Management Cloud	EVL-MC-MSMC	$ -	$ -
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100-499	MC-MSMC-000499-1Y	$ 62.00	$ 53.94
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100-499	MC-MSMC-000499-2Y	$ 124.00	$ 107.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100-499	MC-MSMC-000499-3Y	$ 167.40	$ 145.64
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100-499	MC-MSMC-000499-4Y	$ 223.20	$ 194.18
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 100-499	MC-MSMC-000499-5Y	$ 279.00	$ 242.73
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 500-999	MC-MSMC-000999-1Y	$ 52.00	$ 45.24
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 500-999	MC-MSMC-000999-2Y	$ 104.00	$ 90.48
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 500-999	MC-MSMC-000999-3Y	$ 140.40	$ 122.15
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 500-999	MC-MSMC-000999-4Y	$ 187.20	$ 162.86
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 500-999	MC-MSMC-000999-5Y	$ 234.00	$ 203.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 1000-1999	MC-MSMC-001999-1Y	$ 43.00	$ 37.41
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 1000-1999	MC-MSMC-001999-2Y	$ 86.00	$ 74.82
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 1000-1999	MC-MSMC-001999-3Y	$ 116.10	$ 101.01
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 1000-1999	MC-MSMC-001999-4Y	$ 154.80	$ 134.68
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 1000-1999	MC-MSMC-001999-5Y	$ 193.50	$ 168.35
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 2000-4999	MC-MSMC-004999-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 2000-4999	MC-MSMC-004999-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 2000-4999	MC-MSMC-004999-3Y	$ 97.20	$ 84.56
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 2000-4999	MC-MSMC-004999-4Y	$ 129.60	$ 112.75
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 2000-4999	MC-MSMC-004999-5Y	$ 162.00	$ 140.94
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 5000-9999	MC-MSMC-009999-1Y	$ 30.00	$ 26.10
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 5000-9999	MC-MSMC-009999-2Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 5000-9999	MC-MSMC-009999-3Y	$ 81.00	$ 70.47
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 5000-9999	MC-MSMC-009999-4Y	$ 108.00	$ 93.96
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 5000-9999	MC-MSMC-009999-5Y	$ 135.00	$ 117.45
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 10000-19999	MC-MSMC-019999-1Y	$ 25.00	$ 21.75
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 10000-19999	MC-MSMC-019999-2Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 10000-19999	MC-MSMC-019999-3Y	$ 67.50	$ 58.73
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 10000-19999	MC-MSMC-019999-4Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 10000-19999	MC-MSMC-019999-5Y	$ 112.50	$ 97.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 20000-49999	MC-MSMC-049999-1Y	$ 21.00	$ 18.27
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 20000-49999	MC-MSMC-049999-2Y	$ 42.00	$ 36.54
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 20000-49999	MC-MSMC-049999-3Y	$ 56.70	$ 49.33
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 20000-49999	MC-MSMC-049999-4Y	$ 75.60	$ 65.77
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 20000-49999	MC-MSMC-049999-5Y	$ 94.50	$ 82.22
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 50000-74999	MC-MSMC-074999-1Y	$ 17.00	$ 14.79
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 50000-74999	MC-MSMC-074999-2Y	$ 34.00	$ 29.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 50000-74999	MC-MSMC-074999-3Y	$ 45.90	$ 39.93
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 50000-74999	MC-MSMC-074999-4Y	$ 61.20	$ 53.24
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 50000-74999	MC-MSMC-074999-5Y	$ 76.50	$ 66.56
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 75000-99999	MC-MSMC-099999-1Y	$ 14.00	$ 12.18
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 75000-99999	MC-MSMC-099999-2Y	$ 28.00	$ 24.36
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 75000-99999	MC-MSMC-099999-3Y	$ 37.80	$ 32.89
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 75000-99999	MC-MSMC-099999-4Y	$ 50.40	$ 43.85
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 75000-99999	MC-MSMC-099999-5Y	$ 63.00	$ 54.81

FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100000+	MC-MSMC-100000+1Y	$ 12.00	$ 10.44
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100000+	MC-MSMC-100000+2Y	$ 24.00	$ 20.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100000+	MC-MSMC-100000+3Y	$ 32.40	$ 28.19
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100000+	MC-MSMC-100000+4Y	$ 43.20	$ 37.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 100000+	MC-MSMC-100000+5Y	$ 54.00	$ 46.98
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100-499	RN-MC-MSMC-000499-1Y	$ 62.00	$ 53.94
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100-499	RN-MC-MSMC-000499-2Y	$ 124.00	$ 107.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100-499	RN-MC-MSMC-000499-3Y	$ 167.40	$ 145.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100-499	RN-MC-MSMC-000499-4Y	$ 223.20	$ 194.18
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum	TAP-1KEPS-BD-1Y-P	$ 110,450.00	$ 96,091.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-BD-1Y-P	$ 118,988.00	$ 103,519.56
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum	TAP-5KEPS-BD-1Y-P	$ 121,208.00	$ 105,450.96
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum	TAP-10KEPS-BD-1Y-P	$ 148,132.00	$ 128,874.84
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum	TAP-15KEPS-BD-1Y-P	$ 222,198.00	$ 193,312.26
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum	TAP-20KEPS-BD-1Y-P	$ 265,078.00	$ 230,617.86
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum	TAP-25KEPS-BD-1Y-P	$ 314,780.00	$ 273,858.60
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum	TAP-30KEPS-BD-1Y-P	$ 377,736.00	$ 328,630.32
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum	TAP-35KEPS-BD-1Y-P	$ 440,692.00	$ 383,402.04
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum	TAP-40KEPS-BD-1Y-P	$ 503,648.00	$ 438,173.76
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum	TAP-45KEPS-BD-1Y-P	$ 566,604.00	$ 492,945.48
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum	TAP-50KEPS-BD-1Y-P	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum	TAP-55KEPS-BD-1Y-P	$ 692,516.00	$ 602,488.92
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum	TAP-60KEPS-BD-1Y-P	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum	TAP-65KEPS-BD-1Y-P	$ 818,428.00	$ 712,032.36
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum	TAP-70KEPS-BD-1Y-P	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum	TAP-75KEPS-BD-1Y-P	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum	TAP-80KEPS-BD-1Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum	TAP-1KEPS-BD-2Y-P	$ 220,900.00	$ 192,183.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-BD-2Y-P	$ 237,976.00	$ 207,039.12
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum	TAP-5KEPS-BD-2Y-P	$ 242,416.00	$ 210,901.92
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum	TAP-10KEPS-BD-2Y-P	$ 296,264.00	$ 257,749.68
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum	TAP-15KEPS-BD-2Y-P	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum	TAP-20KEPS-BD-2Y-P	$ 530,156.00	$ 461,235.72
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum	TAP-25KEPS-BD-2Y-P	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum	TAP-30KEPS-BD-2Y-P	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum	TAP-35KEPS-BD-2Y-P	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum	TAP-40KEPS-BD-2Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum	TAP-45KEPS-BD-2Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum	TAP-50KEPS-BD-2Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum	TAP-55KEPS-BD-2Y-P	$ 1,385,032.00	$ 1,204,977.84
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum	TAP-60KEPS-BD-2Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum	TAP-65KEPS-BD-2Y-P	$ 1,636,856.00	$ 1,424,064.72
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum	TAP-70KEPS-BD-2Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum	TAP-75KEPS-BD-2Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum	TAP-80KEPS-BD-2Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum	TAP-1KEPS-BD-3Y-P	$ 331,350.00	$ 288,274.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-BD-3Y-P	$ 356,964.00	$ 310,558.68
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum	TAP-5KEPS-BD-3Y-P	$ 363,624.00	$ 316,352.88
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum	TAP-10KEPS-BD-3Y-P	$ 444,396.00	$ 386,624.52

FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum	TAP-15KEPS-BD-3Y-P	$ 666,594.00	$ 579,936.78
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum	TAP-20KEPS-BD-3Y-P	$ 795,234.00	$ 691,853.58
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum	TAP-25KEPS-BD-3Y-P	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum	TAP-30KEPS-BD-3Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum	TAP-35KEPS-BD-3Y-P	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum	TAP-40KEPS-BD-3Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum	TAP-45KEPS-BD-3Y-P	$ 1,699,812.00	$ 1,478,836.44
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum	TAP-50KEPS-BD-3Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum	TAP-55KEPS-BD-3Y-P	$ 2,077,548.00	$ 1,807,466.76
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum	TAP-60KEPS-BD-3Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum	TAP-65KEPS-BD-3Y-P	$ 2,455,284.00	$ 2,136,097.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum	TAP-70KEPS-BD-3Y-P	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum	TAP-75KEPS-BD-3Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum	TAP-80KEPS-BD-3Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum	TAP-1KEPS-BD-4Y-P	$ 441,800.00	$ 384,366.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-BD-4Y-P	$ 475,952.00	$ 414,078.24
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum	TAP-5KEPS-BD-4Y-P	$ 484,832.00	$ 421,803.84
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum	TAP-10KEPS-BD-4Y-P	$ 592,528.00	$ 515,499.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum	TAP-15KEPS-BD-4Y-P	$ 888,792.00	$ 773,249.04
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum	TAP-20KEPS-BD-4Y-P	$ 1,060,312.00	$ 922,471.44
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum	TAP-25KEPS-BD-4Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum	TAP-30KEPS-BD-4Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum	TAP-35KEPS-BD-4Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum	TAP-40KEPS-BD-4Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum	TAP-45KEPS-BD-4Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum	TAP-50KEPS-BD-4Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum	TAP-55KEPS-BD-4Y-P	$ 2,770,064.00	$ 2,409,955.68
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum	TAP-60KEPS-BD-4Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum	TAP-65KEPS-BD-4Y-P	$ 3,273,712.00	$ 2,848,129.44
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum	TAP-70KEPS-BD-4Y-P	$ 3,525,536.00	$ 3,067,216.32
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum	TAP-75KEPS-BD-4Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum	TAP-80KEPS-BD-4Y-P	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Platinum	TAP-1KEPS-BD-5Y-P	$ 552,250.00	$ 480,457.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-BD-5Y-P	$ 594,940.00	$ 517,597.80
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Platinum	TAP-5KEPS-BD-5Y-P	$ 606,040.00	$ 527,254.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Platinum	TAP-10KEPS-BD-5Y-P	$ 740,660.00	$ 644,374.20
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Platinum	TAP-15KEPS-BD-5Y-P	$ 1,110,990.00	$ 966,561.30
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Platinum	TAP-20KEPS-BD-5Y-P	$ 1,325,390.00	$ 1,153,089.30
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Platinum	TAP-25KEPS-BD-5Y-P	$ 1,573,900.00	$ 1,369,293.00
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Platinum	TAP-30KEPS-BD-5Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Platinum	TAP-35KEPS-BD-5Y-P	$ 2,203,460.00	$ 1,917,010.20
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Platinum	TAP-40KEPS-BD-5Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Platinum	TAP-45KEPS-BD-5Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Platinum	TAP-50KEPS-BD-5Y-P	$ 3,147,800.00	$ 2,738,586.00
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Platinum	TAP-55KEPS-BD-5Y-P	$ 3,462,580.00	$ 3,012,444.60
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Platinum	TAP-60KEPS-BD-5Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Platinum	TAP-65KEPS-BD-5Y-P	$ 4,092,140.00	$ 3,560,161.80
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Platinum	TAP-70KEPS-BD-5Y-P	$ 4,406,920.00	$ 3,834,020.40
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Platinum	TAP-75KEPS-BD-5Y-P	$ 4,721,700.00	$ 4,107,879.00

FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Platinum	TAP-80KEPS-BD-5Y-P	$ 5,036,480.00	$ 4,381,737.60
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-BD-1Y-P	$ 110,450.00	$ 96,091.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-BD-1Y-P	$ 118,988.00	$ 103,519.56
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-BD-1Y-P	$ 121,208.00	$ 105,450.96
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-BD-1Y-P	$ 148,132.00	$ 128,874.84
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-BD-1Y-P	$ 222,198.00	$ 193,312.26
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-BD-1Y-P	$ 265,078.00	$ 230,617.86
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-BD-1Y-P	$ 314,780.00	$ 273,858.60
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-BD-1Y-P	$ 377,736.00	$ 328,630.32
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-BD-1Y-P	$ 440,692.00	$ 383,402.04
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-BD-1Y-P	$ 503,648.00	$ 438,173.76
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum	RN-TAP-45KEPS-BD-1Y-P	$ 566,604.00	$ 492,945.48
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum	RN-TAP-50KEPS-BD-1Y-P	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum	RN-TAP-55KEPS-BD-1Y-P	$ 692,516.00	$ 602,488.92
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum	RN-TAP-60KEPS-BD-1Y-P	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum	RN-TAP-65KEPS-BD-1Y-P	$ 818,428.00	$ 712,032.36
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum	RN-TAP-70KEPS-BD-1Y-P	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum	RN-TAP-75KEPS-BD-1Y-P	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum	RN-TAP-80KEPS-BD-1Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-BD-2Y-P	$ 220,900.00	$ 192,183.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-BD-2Y-P	$ 237,976.00	$ 207,039.12
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-BD-2Y-P	$ 242,416.00	$ 210,901.92
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-BD-2Y-P	$ 296,264.00	$ 257,749.68
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-BD-2Y-P	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-BD-2Y-P	$ 530,156.00	$ 461,235.72
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-BD-2Y-P	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-BD-2Y-P	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-BD-2Y-P	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-BD-2Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum	RN-TAP-45KEPS-BD-2Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum	RN-TAP-50KEPS-BD-2Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum	RN-TAP-55KEPS-BD-2Y-P	$ 1,385,032.00	$ 1,204,977.84
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum	RN-TAP-60KEPS-BD-2Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum	RN-TAP-65KEPS-BD-2Y-P	$ 1,636,856.00	$ 1,424,064.72
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum	RN-TAP-70KEPS-BD-2Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum	RN-TAP-75KEPS-BD-2Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum	RN-TAP-80KEPS-BD-2Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-BD-3Y-P	$ 331,350.00	$ 288,274.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-BD-3Y-P	$ 356,964.00	$ 310,558.68
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-BD-3Y-P	$ 363,624.00	$ 316,352.88
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-BD-3Y-P	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-BD-3Y-P	$ 666,594.00	$ 579,936.78
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-BD-3Y-P	$ 795,234.00	$ 691,853.58
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-BD-3Y-P	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-BD-3Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-BD-3Y-P	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-BD-3Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum	RN-TAP-45KEPS-BD-3Y-P	$ 1,699,812.00	$ 1,478,836.44
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum	RN-TAP-50KEPS-BD-3Y-P	$ 1,888,680.00	$ 1,643,151.60

FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum	RN-TAP-55KEPS-BD-3Y-P	$ 2,077,548.00	$ 1,807,466.76
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum	RN-TAP-60KEPS-BD-3Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum	RN-TAP-65KEPS-BD-3Y-P	$ 2,455,284.00	$ 2,136,097.08
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum	RN-TAP-70KEPS-BD-3Y-P	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum	RN-TAP-75KEPS-BD-3Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum	RN-TAP-80KEPS-BD-3Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-BD-4Y-P	$ 441,800.00	$ 384,366.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-BD-4Y-P	$ 475,952.00	$ 414,078.24
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-BD-4Y-P	$ 484,832.00	$ 421,803.84
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-BD-4Y-P	$ 592,528.00	$ 515,499.36
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-BD-4Y-P	$ 888,792.00	$ 773,249.04
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-BD-4Y-P	$ 1,060,312.00	$ 922,471.44
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-BD-4Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-BD-4Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-BD-4Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-BD-4Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum	RN-TAP-45KEPS-BD-4Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum	RN-TAP-50KEPS-BD-4Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum	RN-TAP-55KEPS-BD-4Y-P	$ 2,770,064.00	$ 2,409,955.68
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum	RN-TAP-60KEPS-BD-4Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum	RN-TAP-65KEPS-BD-4Y-P	$ 3,273,712.00	$ 2,848,129.44
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum	RN-TAP-70KEPS-BD-4Y-P	$ 3,525,536.00	$ 3,067,216.32
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum	RN-TAP-75KEPS-BD-4Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum	RN-TAP-80KEPS-BD-4Y-P	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-BD-1Y-PPP	$ 115,973.00	$ 100,896.51
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-BD-1Y-PPP	$ 124,937.00	$ 108,695.19
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-BD-1Y-PPP	$ 127,268.00	$ 110,723.16
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-BD-1Y-PPP	$ 155,539.00	$ 135,318.93
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-BD-1Y-PPP	$ 233,308.00	$ 202,977.96
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-BD-1Y-PPP	$ 278,332.00	$ 242,148.84
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-BD-1Y-PPP	$ 330,519.00	$ 287,551.53
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-BD-1Y-PPP	$ 396,623.00	$ 345,062.01
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-BD-1Y-PPP	$ 462,727.00	$ 402,572.49
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-BD-1Y-PPP	$ 528,830.00	$ 460,082.10
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-BD-1Y-PPP	$ 594,934.00	$ 517,592.58
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-BD-1Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-BD-1Y-PPP	$ 727,142.00	$ 632,613.54
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-BD-1Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-BD-1Y-PPP	$ 859,349.00	$ 747,633.63
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-BD-1Y-PPP	$ 925,453.00	$ 805,144.11
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-BD-1Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-BD-1Y-PPP	$ 1,057,661.00	$ 920,165.07
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-BD-2Y-PPP	$ 231,946.00	$ 201,793.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-BD-2Y-PPP	$ 249,874.00	$ 217,390.38
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-BD-2Y-PPP	$ 254,536.00	$ 221,446.32
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-BD-2Y-PPP	$ 311,078.00	$ 270,637.86
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-BD-2Y-PPP	$ 466,616.00	$ 405,955.92
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-BD-2Y-PPP	$ 556,664.00	$ 484,297.68
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-BD-2Y-PPP	$ 661,038.00	$ 575,103.06

FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-BD-2Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-BD-2Y-PPP	$ 925,454.00	$ 805,144.98
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-BD-2Y-PPP	$ 1,057,660.00	$ 920,164.20
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-BD-2Y-PPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-BD-2Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-BD-2Y-PPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-BD-2Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-BD-2Y-PPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-BD-2Y-PPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-BD-2Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-BD-2Y-PPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-BD-3Y-PPP	$ 347,919.00	$ 302,689.53
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-BD-3Y-PPP	$ 374,811.00	$ 326,085.57
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-BD-3Y-PPP	$ 381,804.00	$ 332,169.48
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-BD-3Y-PPP	$ 466,617.00	$ 405,956.79
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-BD-3Y-PPP	$ 699,924.00	$ 608,933.88
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-BD-3Y-PPP	$ 834,996.00	$ 726,446.52
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-BD-3Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-BD-3Y-PPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-BD-3Y-PPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-BD-3Y-PPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-BD-3Y-PPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-BD-3Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-BD-3Y-PPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-BD-3Y-PPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-BD-3Y-PPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-BD-3Y-PPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-BD-3Y-PPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-BD-3Y-PPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-BD-4Y-PPP	$ 463,892.00	$ 403,586.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-BD-4Y-PPP	$ 499,748.00	$ 434,780.76
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-BD-4Y-PPP	$ 509,072.00	$ 442,892.64
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-BD-4Y-PPP	$ 622,156.00	$ 541,275.72
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-BD-4Y-PPP	$ 933,232.00	$ 811,911.84
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-BD-4Y-PPP	$ 1,113,328.00	$ 968,595.36
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-BD-4Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-BD-4Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-BD-4Y-PPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-BD-4Y-PPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-BD-4Y-PPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-BD-4Y-PPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-BD-4Y-PPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-BD-4Y-PPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-BD-4Y-PPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-BD-4Y-PPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-BD-4Y-PPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-BD-4Y-PPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-BD-5Y-PPP	$ 579,865.00	$ 504,482.55
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-BD-5Y-PPP	$ 624,685.00	$ 543,475.95

FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-BD-5Y-PPP	$ 636,340.00	$ 553,615.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-BD-5Y-PPP	$ 777,695.00	$ 676,594.65
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-BD-5Y-PPP	$ 1,166,540.00	$ 1,014,889.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-BD-5Y-PPP	$ 1,391,660.00	$ 1,210,744.20
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-BD-5Y-PPP	$ 1,652,595.00	$ 1,437,757.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-BD-5Y-PPP	$ 1,983,115.00	$ 1,725,310.05
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-BD-5Y-PPP	$ 2,313,635.00	$ 2,012,862.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-BD-5Y-PPP	$ 2,644,150.00	$ 2,300,410.50
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-BD-5Y-PPP	$ 2,974,670.00	$ 2,587,962.90
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-BD-5Y-PPP	$ 3,305,190.00	$ 2,875,515.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-BD-5Y-PPP	$ 3,635,710.00	$ 3,163,067.70
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-BD-5Y-PPP	$ 3,966,230.00	$ 3,450,620.10
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-BD-5Y-PPP	$ 4,296,745.00	$ 3,738,168.15
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-BD-5Y-PPP	$ 4,627,265.00	$ 4,025,720.55
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-BD-5Y-PPP	$ 4,957,785.00	$ 4,313,272.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-BD-5Y-PPP	$ 5,288,305.00	$ 4,600,825.35
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-BD-1Y-PPP	$ 115,973.00	$ 100,896.51
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-1Y-PPP	$ 124,937.00	$ 108,695.19
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-BD-1Y-PPP	$ 127,268.00	$ 110,723.16
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-BD-1Y-PPP	$ 155,539.00	$ 135,318.93
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-BD-1Y-PPP	$ 233,308.00	$ 202,977.96
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-BD-1Y-PPP	$ 278,332.00	$ 242,148.84
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-BD-1Y-PPP	$ 330,519.00	$ 287,551.53
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-BD-1Y-PPP	$ 396,623.00	$ 345,062.01
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-BD-1Y-PPP	$ 462,727.00	$ 402,572.49
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-BD-1Y-PPP	$ 528,830.00	$ 460,082.10
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - Plat Prio Plus	RN-TAP-45KEPS-BD-1Y-PPP	$ 594,934.00	$ 517,592.58
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - Plat Prio Plus	RN-TAP-50KEPS-BD-1Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - Plat Prio Plus	RN-TAP-55KEPS-BD-1Y-PPP	$ 727,142.00	$ 632,613.54
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - Plat Prio Plus	RN-TAP-60KEPS-BD-1Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - Plat Prio Plus	RN-TAP-65KEPS-BD-1Y-PPP	$ 859,349.00	$ 747,633.63
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - Plat Prio Plus	RN-TAP-70KEPS-BD-1Y-PPP	$ 925,453.00	$ 805,144.11
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - Plat Prio Plus	RN-TAP-75KEPS-BD-1Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - Plat Prio Plus	RN-TAP-80KEPS-BD-1Y-PPP	$ 1,057,661.00	$ 920,165.07
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-BD-2Y-PPP	$ 231,946.00	$ 201,793.02
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-2Y-PPP	$ 249,874.00	$ 217,390.38
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-BD-2Y-PPP	$ 254,536.00	$ 221,446.32
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-BD-2Y-PPP	$ 311,078.00	$ 270,637.86
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-BD-2Y-PPP	$ 466,616.00	$ 405,955.92
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-BD-2Y-PPP	$ 556,664.00	$ 484,297.68
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-BD-2Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-BD-2Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-BD-2Y-PPP	$ 925,454.00	$ 805,144.98
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-BD-2Y-PPP	$ 1,057,660.00	$ 920,164.20
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - Plat Prio Plus	RN-TAP-45KEPS-BD-2Y-PPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - Plat Prio Plus	RN-TAP-50KEPS-BD-2Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - Plat Prio Plus	RN-TAP-55KEPS-BD-2Y-PPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - Plat Prio Plus	RN-TAP-60KEPS-BD-2Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - Plat Prio Plus	RN-TAP-65KEPS-BD-2Y-PPP	$ 1,718,698.00	$ 1,495,267.26

FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - Plat Prio Plus	RN-TAP-70KEPS-BD-2Y-PPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - Plat Prio Plus	RN-TAP-75KEPS-BD-2Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - Plat Prio Plus	RN-TAP-80KEPS-BD-2Y-PPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-BD-3Y-PPP	$ 347,919.00	$ 302,689.53
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-3Y-PPP	$ 374,811.00	$ 326,085.57
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-BD-3Y-PPP	$ 381,804.00	$ 332,169.48
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-BD-3Y-PPP	$ 466,617.00	$ 405,956.79
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-BD-3Y-PPP	$ 699,924.00	$ 608,933.88
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-BD-3Y-PPP	$ 834,996.00	$ 726,446.52
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-BD-3Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-BD-3Y-PPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-BD-3Y-PPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-BD-3Y-PPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - Plat Prio Plus	RN-TAP-45KEPS-BD-3Y-PPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - Plat Prio Plus	RN-TAP-50KEPS-BD-3Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - Plat Prio Plus	RN-TAP-55KEPS-BD-3Y-PPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - Plat Prio Plus	RN-TAP-60KEPS-BD-3Y-PPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - Plat Prio Plus	RN-TAP-65KEPS-BD-3Y-PPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - Plat Prio Plus	RN-TAP-70KEPS-BD-3Y-PPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - Plat Prio Plus	RN-TAP-75KEPS-BD-3Y-PPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - Plat Prio Plus	RN-TAP-80KEPS-BD-3Y-PPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-BD-4Y-PPP	$ 463,892.00	$ 403,586.04
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-4Y-PPP	$ 499,748.00	$ 434,780.76
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-BD-4Y-PPP	$ 509,072.00	$ 442,892.64
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-BD-4Y-PPP	$ 622,156.00	$ 541,275.72
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-BD-4Y-PPP	$ 933,232.00	$ 811,911.84
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-BD-4Y-PPP	$ 1,113,328.00	$ 968,595.36
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-BD-4Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-BD-4Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-BD-4Y-PPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-BD-4Y-PPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - Plat Prio Plus	RN-TAP-45KEPS-BD-4Y-PPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - Plat Prio Plus	RN-TAP-50KEPS-BD-4Y-PPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - Plat Prio Plus	RN-TAP-55KEPS-BD-4Y-PPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - Plat Prio Plus	RN-TAP-60KEPS-BD-4Y-PPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - Plat Prio Plus	RN-TAP-65KEPS-BD-4Y-PPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - Plat Prio Plus	RN-TAP-70KEPS-BD-4Y-PPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - Plat Prio Plus	RN-TAP-75KEPS-BD-4Y-PPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - Plat Prio Plus	RN-TAP-80KEPS-BD-4Y-PPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum	TAP-1KEPS-SS-1Y-P	$ 232,635.00	$ 202,392.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-SS-1Y-P	$ 276,258.00	$ 240,344.46
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum	TAP-5KEPS-SS-1Y-P	$ 314,613.00	$ 273,713.31
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum	TAP-10KEPS-SS-1Y-P	$ 475,966.00	$ 414,090.42
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum	TAP-15KEPS-SS-1Y-P	$ 713,949.00	$ 621,135.63
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum	TAP-20KEPS-SS-1Y-P	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum	TAP-25KEPS-SS-1Y-P	$ 1,189,915.00	$ 1,035,226.05
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum	TAP-30KEPS-SS-1Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum	TAP-35KEPS-SS-1Y-P	$ 1,665,881.00	$ 1,449,316.47
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum	TAP-40KEPS-SS-1Y-P	$ 1,903,864.00	$ 1,656,361.68

FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum	TAP-45KEPS-SS-1Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum	TAP-50KEPS-SS-1Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum	TAP-55KEPS-SS-1Y-P	$ 2,617,813.00	$ 2,277,497.31
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum	TAP-60KEPS-SS-1Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum	TAP-65KEPS-SS-1Y-P	$ 3,093,779.00	$ 2,691,587.73
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum	TAP-70KEPS-SS-1Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum	TAP-75KEPS-SS-1Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum	TAP-80KEPS-SS-1Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum	TAP-1KEPS-SS-2Y-P	$ 465,270.00	$ 404,784.90
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-SS-2Y-P	$ 552,516.00	$ 480,688.92
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum	TAP-5KEPS-SS-2Y-P	$ 629,226.00	$ 547,426.62
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum	TAP-10KEPS-SS-2Y-P	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum	TAP-15KEPS-SS-2Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum	TAP-20KEPS-SS-2Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum	TAP-25KEPS-SS-2Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum	TAP-30KEPS-SS-2Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum	TAP-35KEPS-SS-2Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum	TAP-40KEPS-SS-2Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum	TAP-45KEPS-SS-2Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum	TAP-50KEPS-SS-2Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum	TAP-55KEPS-SS-2Y-P	$ 5,235,626.00	$ 4,554,994.62
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum	TAP-60KEPS-SS-2Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum	TAP-65KEPS-SS-2Y-P	$ 6,187,558.00	$ 5,383,175.46
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum	TAP-70KEPS-SS-2Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum	TAP-75KEPS-SS-2Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum	TAP-80KEPS-SS-2Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum	TAP-1KEPS-SS-3Y-P	$ 697,905.00	$ 607,177.35
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-SS-3Y-P	$ 828,774.00	$ 721,033.38
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum	TAP-5KEPS-SS-3Y-P	$ 943,839.00	$ 821,139.93
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum	TAP-10KEPS-SS-3Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum	TAP-15KEPS-SS-3Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum	TAP-20KEPS-SS-3Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum	TAP-25KEPS-SS-3Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum	TAP-30KEPS-SS-3Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum	TAP-35KEPS-SS-3Y-P	$ 4,997,643.00	$ 4,347,949.41
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum	TAP-40KEPS-SS-3Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum	TAP-45KEPS-SS-3Y-P	$ 6,425,541.00	$ 5,590,220.67
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum	TAP-50KEPS-SS-3Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum	TAP-55KEPS-SS-3Y-P	$ 7,853,439.00	$ 6,832,491.93
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum	TAP-60KEPS-SS-3Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum	TAP-65KEPS-SS-3Y-P	$ 9,281,337.00	$ 8,074,763.19
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum	TAP-70KEPS-SS-3Y-P	$ 9,995,286.00	$ 8,695,898.82
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum	TAP-75KEPS-SS-3Y-P	##############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum	TAP-80KEPS-SS-3Y-P	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum	TAP-1KEPS-SS-4Y-P	$ 930,540.00	$ 809,569.80
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-SS-4Y-P	$ 1,105,032.00	$ 961,377.84
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum	TAP-5KEPS-SS-4Y-P	$ 1,258,452.00	$ 1,094,853.24
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum	TAP-10KEPS-SS-4Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum	TAP-15KEPS-SS-4Y-P	$ 2,855,796.00	$ 2,484,542.52

FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum	TAP-20KEPS-SS-4Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum	TAP-25KEPS-SS-4Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum	TAP-30KEPS-SS-4Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum	TAP-35KEPS-SS-4Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum	TAP-40KEPS-SS-4Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum	TAP-45KEPS-SS-4Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum	TAP-50KEPS-SS-4Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum	TAP-55KEPS-SS-4Y-P	############	$ 9,109,989.24
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum	TAP-60KEPS-SS-4Y-P	############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum	TAP-65KEPS-SS-4Y-P	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum	TAP-70KEPS-SS-4Y-P	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum	TAP-75KEPS-SS-4Y-P	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum	TAP-80KEPS-SS-4Y-P	############	############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Platinum	TAP-1KEPS-SS-5Y-P	$ 1,163,175.00	$ 1,011,962.25
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-SS-5Y-P	$ 1,381,290.00	$ 1,201,722.30
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Platinum	TAP-5KEPS-SS-5Y-P	$ 1,573,065.00	$ 1,368,566.55
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Platinum	TAP-10KEPS-SS-5Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Platinum	TAP-15KEPS-SS-5Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Platinum	TAP-20KEPS-SS-5Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Platinum	TAP-25KEPS-SS-5Y-P	$ 5,949,575.00	$ 5,176,130.25
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Platinum	TAP-30KEPS-SS-5Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Platinum	TAP-35KEPS-SS-5Y-P	$ 8,329,405.00	$ 7,246,582.35
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Platinum	TAP-40KEPS-SS-5Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Platinum	TAP-45KEPS-SS-5Y-P	############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Platinum	TAP-50KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Platinum	TAP-55KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Platinum	TAP-60KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Platinum	TAP-65KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Platinum	TAP-70KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Platinum	TAP-75KEPS-SS-5Y-P	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Platinum	TAP-80KEPS-SS-5Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-SS-1Y-P	$ 232,635.00	$ 202,392.45
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-SS-1Y-P	$ 276,258.00	$ 240,344.46
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-SS-1Y-P	$ 314,613.00	$ 273,713.31
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-SS-1Y-P	$ 475,966.00	$ 414,090.42
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-SS-1Y-P	$ 713,949.00	$ 621,135.63
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-SS-1Y-P	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-SS-1Y-P	$ 1,189,915.00	$ 1,035,226.05
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-SS-1Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-SS-1Y-P	$ 1,665,881.00	$ 1,449,316.47
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-SS-1Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum	RN-TAP-45KEPS-SS-1Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum	RN-TAP-50KEPS-SS-1Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum	RN-TAP-55KEPS-SS-1Y-P	$ 2,617,813.00	$ 2,277,497.31
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum	RN-TAP-60KEPS-SS-1Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum	RN-TAP-65KEPS-SS-1Y-P	$ 3,093,779.00	$ 2,691,587.73
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum	RN-TAP-70KEPS-SS-1Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum	RN-TAP-75KEPS-SS-1Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum	RN-TAP-80KEPS-SS-1Y-P	$ 3,807,728.00	$ 3,312,723.36

FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-SS-2Y-P	$ 465,270.00	$ 404,784.90
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-SS-2Y-P	$ 552,516.00	$ 480,688.92
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-SS-2Y-P	$ 629,226.00	$ 547,426.62
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-SS-2Y-P	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-SS-2Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-SS-2Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-SS-2Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-SS-2Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-SS-2Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-SS-2Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum	RN-TAP-45KEPS-SS-2Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum	RN-TAP-50KEPS-SS-2Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum	RN-TAP-55KEPS-SS-2Y-P	$ 5,235,626.00	$ 4,554,994.62
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum	RN-TAP-60KEPS-SS-2Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum	RN-TAP-65KEPS-SS-2Y-P	$ 6,187,558.00	$ 5,383,175.46
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum	RN-TAP-70KEPS-SS-2Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum	RN-TAP-75KEPS-SS-2Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum	RN-TAP-80KEPS-SS-2Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-SS-3Y-P	$ 697,905.00	$ 607,177.35
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-SS-3Y-P	$ 828,774.00	$ 721,033.38
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-SS-3Y-P	$ 943,839.00	$ 821,139.93
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-SS-3Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-SS-3Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-SS-3Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-SS-3Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-SS-3Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-SS-3Y-P	$ 4,997,643.00	$ 4,347,949.41
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-SS-3Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum	RN-TAP-45KEPS-SS-3Y-P	$ 6,425,541.00	$ 5,590,220.67
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum	RN-TAP-50KEPS-SS-3Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum	RN-TAP-55KEPS-SS-3Y-P	$ 7,853,439.00	$ 6,832,491.93
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum	RN-TAP-60KEPS-SS-3Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum	RN-TAP-65KEPS-SS-3Y-P	$ 9,281,337.00	$ 8,074,763.19
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum	RN-TAP-70KEPS-SS-3Y-P	$ 9,995,286.00	$ 8,695,898.82
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum	RN-TAP-75KEPS-SS-3Y-P	##############	$ 9,317,034.45
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum	RN-TAP-80KEPS-SS-3Y-P	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-SS-4Y-P	$ 930,540.00	$ 809,569.80
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-SS-4Y-P	$ 1,105,032.00	$ 961,377.84
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-SS-4Y-P	$ 1,258,452.00	$ 1,094,853.24
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-SS-4Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-SS-4Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-SS-4Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-SS-4Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-SS-4Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-SS-4Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-SS-4Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum	RN-TAP-45KEPS-SS-4Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum	RN-TAP-50KEPS-SS-4Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum	RN-TAP-55KEPS-SS-4Y-P	##############	$ 9,109,989.24

FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum	RN-TAP-60KEPS-SS-4Y-P	##########	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum	RN-TAP-65KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum	RN-TAP-70KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum	RN-TAP-75KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum	RN-TAP-80KEPS-SS-4Y-P	##########	##########
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-SS-1Y-PPP	$ 244,267.00	$ 212,512.29
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-SS-1Y-PPP	$ 290,071.00	$ 252,361.77
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-SS-1Y-PPP	$ 330,344.00	$ 287,399.28
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-SS-1Y-PPP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-SS-1Y-PPP	$ 749,646.00	$ 652,192.02
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-SS-1Y-PPP	$ 999,529.00	$ 869,590.23
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-SS-1Y-PPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-SS-1Y-PPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-SS-1Y-PPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-SS-1Y-PPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-SS-1Y-PPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-SS-1Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-SS-1Y-PPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-SS-1Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-SS-1Y-PPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-SS-1Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-SS-1Y-PPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-SS-1Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-SS-2Y-PPP	$ 488,534.00	$ 425,024.58
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-SS-2Y-PPP	$ 580,142.00	$ 504,723.54
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-SS-2Y-PPP	$ 660,688.00	$ 574,798.56
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-SS-2Y-PPP	$ 999,528.00	$ 869,589.36
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-SS-2Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-SS-2Y-PPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-SS-2Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-SS-2Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-SS-2Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-SS-2Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-SS-2Y-PPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-SS-2Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-SS-2Y-PPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-SS-2Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-SS-2Y-PPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-SS-2Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-SS-2Y-PPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-SS-2Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-SS-3Y-PPP	$ 732,801.00	$ 637,536.87
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-SS-3Y-PPP	$ 870,213.00	$ 757,085.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-SS-3Y-PPP	$ 991,032.00	$ 862,197.84
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-SS-3Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-SS-3Y-PPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-SS-3Y-PPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-SS-3Y-PPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-SS-3Y-PPP	$ 4,497,879.00	$ 3,913,154.73

FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-SS-3Y-PPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-SS-3Y-PPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-SS-3Y-PPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-SS-3Y-PPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-SS-3Y-PPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-SS-3Y-PPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-SS-3Y-PPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-SS-3Y-PPP	############	$ 9,130,693.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-SS-3Y-PPP	############	$ 9,782,885.52
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-SS-3Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-SS-4Y-PPP	$ 977,068.00	$ 850,049.16
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-SS-4Y-PPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-SS-4Y-PPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-SS-4Y-PPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-SS-4Y-PPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-SS-4Y-PPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-SS-4Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-SS-4Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-SS-4Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-SS-4Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-SS-4Y-PPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-SS-4Y-PPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-SS-4Y-PPP	############	$ 9,565,489.92
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-SS-5Y-PPP	$ 1,221,335.00	$ 1,062,561.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-SS-5Y-PPP	$ 1,450,355.00	$ 1,261,808.85
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-SS-5Y-PPP	$ 1,651,720.00	$ 1,436,996.40
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-SS-5Y-PPP	$ 2,498,820.00	$ 2,173,973.40
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-SS-5Y-PPP	$ 3,748,230.00	$ 3,260,960.10
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-SS-5Y-PPP	$ 4,997,645.00	$ 4,347,951.15
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-SS-5Y-PPP	$ 6,247,055.00	$ 5,434,937.85
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-SS-5Y-PPP	$ 7,496,465.00	$ 6,521,924.55
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-SS-5Y-PPP	$ 8,745,875.00	$ 7,608,911.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-SS-5Y-PPP	$ 9,995,285.00	$ 8,695,897.95
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-SS-5Y-PPP	############	$ 9,782,884.65
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-SS-5Y-PPP	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-SS-5Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-SS-1Y-PPP	$ 244,267.00	$ 212,512.29
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-1Y-PPP	$ 290,071.00	$ 252,361.77
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-SS-1Y-PPP	$ 330,344.00	$ 287,399.28

FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-SS-1Y-PPP	$ 499,764.00	$ 434,794.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-SS-1Y-PPP	$ 749,646.00	$ 652,192.02
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-SS-1Y-PPP	$ 999,529.00	$ 869,590.23
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-SS-1Y-PPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-SS-1Y-PPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-SS-1Y-PPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-SS-1Y-PPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - Plat Prio Plus	RN-TAP-45KEPS-SS-1Y-PPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - Plat Prio Plus	RN-TAP-50KEPS-SS-1Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - Plat Prio Plus	RN-TAP-55KEPS-SS-1Y-PPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - Plat Prio Plus	RN-TAP-60KEPS-SS-1Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - Plat Prio Plus	RN-TAP-65KEPS-SS-1Y-PPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - Plat Prio Plus	RN-TAP-70KEPS-SS-1Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - Plat Prio Plus	RN-TAP-75KEPS-SS-1Y-PPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - Plat Prio Plus	RN-TAP-80KEPS-SS-1Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-SS-2Y-PPP	$ 488,534.00	$ 425,024.58
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-2Y-PPP	$ 580,142.00	$ 504,723.54
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-SS-2Y-PPP	$ 660,688.00	$ 574,798.56
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-SS-2Y-PPP	$ 999,528.00	$ 869,589.36
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-SS-2Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-SS-2Y-PPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-SS-2Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-SS-2Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-SS-2Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-SS-2Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - Plat Prio Plus	RN-TAP-45KEPS-SS-2Y-PPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - Plat Prio Plus	RN-TAP-50KEPS-SS-2Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - Plat Prio Plus	RN-TAP-55KEPS-SS-2Y-PPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - Plat Prio Plus	RN-TAP-60KEPS-SS-2Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - Plat Prio Plus	RN-TAP-65KEPS-SS-2Y-PPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - Plat Prio Plus	RN-TAP-70KEPS-SS-2Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - Plat Prio Plus	RN-TAP-75KEPS-SS-2Y-PPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - Plat Prio Plus	RN-TAP-80KEPS-SS-2Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-SS-3Y-PPP	$ 732,801.00	$ 637,536.87
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-3Y-PPP	$ 870,213.00	$ 757,085.31
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-SS-3Y-PPP	$ 991,032.00	$ 862,197.84
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-SS-3Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-SS-3Y-PPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-SS-3Y-PPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-SS-3Y-PPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-SS-3Y-PPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-SS-3Y-PPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-SS-3Y-PPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - Plat Prio Plus	RN-TAP-45KEPS-SS-3Y-PPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - Plat Prio Plus	RN-TAP-50KEPS-SS-3Y-PPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - Plat Prio Plus	RN-TAP-55KEPS-SS-3Y-PPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - Plat Prio Plus	RN-TAP-60KEPS-SS-3Y-PPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - Plat Prio Plus	RN-TAP-65KEPS-SS-3Y-PPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - Plat Prio Plus	RN-TAP-70KEPS-SS-3Y-PPP	##############	$ 9,130,693.50

FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - Plat Prio Plus	RN-TAP-75KEPS-SS-3Y-PPP	############	$ 9,782,885.52
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - Plat Prio Plus	RN-TAP-80KEPS-SS-3Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-SS-4Y-PPP	$ 977,068.00	$ 850,049.16
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-4Y-PPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-SS-4Y-PPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-SS-4Y-PPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-SS-4Y-PPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-SS-4Y-PPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-SS-4Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-SS-4Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-SS-4Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-SS-4Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - Plat Prio Plus	RN-TAP-45KEPS-SS-4Y-PPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - Plat Prio Plus	RN-TAP-50KEPS-SS-4Y-PPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - Plat Prio Plus	RN-TAP-55KEPS-SS-4Y-PPP	############	$ 9,565,489.92
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - Plat Prio Plus	RN-TAP-60KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - Plat Prio Plus	RN-TAP-65KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - Plat Prio Plus	RN-TAP-70KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - Plat Prio Plus	RN-TAP-75KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - Plat Prio Plus	RN-TAP-80KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-LS-1Y-P	$ 492,411.00	$ 428,397.57
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-LS-1Y-P	$ 600,978.00	$ 522,850.86
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-LS-1Y-P	$ 704,277.00	$ 612,720.99
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-LS-1Y-P	$ 1,125,406.00	$ 979,103.22
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-LS-1Y-P	$ 1,688,109.00	$ 1,468,654.83
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-LS-1Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-LS-1Y-P	$ 2,813,515.00	$ 2,447,758.05
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-LS-1Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-LS-1Y-P	$ 3,938,921.00	$ 3,426,861.27
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-LS-1Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-LS-2Y-P	$ 984,822.00	$ 856,795.14
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-LS-2Y-P	$ 1,201,956.00	$ 1,045,701.72
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-LS-2Y-P	$ 1,408,554.00	$ 1,225,441.98
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-LS-2Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-LS-2Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-LS-2Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-LS-2Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-LS-2Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-LS-2Y-P	$ 7,877,842.00	$ 6,853,722.54
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-LS-2Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-LS-3Y-P	$ 1,477,233.00	$ 1,285,192.71
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-LS-3Y-P	$ 1,802,934.00	$ 1,568,552.58
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-LS-3Y-P	$ 2,112,831.00	$ 1,838,162.97
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-LS-3Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-LS-3Y-P	$ 5,064,327.00	$ 4,405,964.49
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-LS-3Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-LS-3Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-LS-3Y-P	############	$ 8,811,928.98
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-LS-3Y-P	############	############

FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-LS-3Y-P	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-LS-4Y-P	$ 1,969,644.00	$ 1,713,590.28
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-LS-4Y-P	$ 2,403,912.00	$ 2,091,403.44
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-LS-4Y-P	$ 2,817,108.00	$ 2,450,883.96
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-LS-4Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-LS-4Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-LS-4Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-LS-4Y-P	############	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-LS-5Y-P	$ 2,462,055.00	$ 2,141,987.85
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-LS-5Y-P	$ 3,004,890.00	$ 2,614,254.30
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-LS-5Y-P	$ 3,521,385.00	$ 3,063,604.95
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-LS-5Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-LS-5Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-LS-5Y-P	############	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-LS-5Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-LS-1Y-P	$ 492,411.00	$ 428,397.57
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-LS-1Y-P	$ 600,978.00	$ 522,850.86
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-LS-1Y-P	$ 704,277.00	$ 612,720.99
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-LS-1Y-P	$ 1,125,406.00	$ 979,103.22
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-LS-1Y-P	$ 1,688,109.00	$ 1,468,654.83
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-LS-1Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-LS-1Y-P	$ 2,813,515.00	$ 2,447,758.05
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-LS-1Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-LS-1Y-P	$ 3,938,921.00	$ 3,426,861.27
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-LS-1Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-LS-2Y-P	$ 984,822.00	$ 856,795.14
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-LS-2Y-P	$ 1,201,956.00	$ 1,045,701.72
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-LS-2Y-P	$ 1,408,554.00	$ 1,225,441.98
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-LS-2Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-LS-2Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-LS-2Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-LS-2Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-LS-2Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-LS-2Y-P	$ 7,877,842.00	$ 6,853,722.54
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-LS-2Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-LS-3Y-P	$ 1,477,233.00	$ 1,285,192.71
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-LS-3Y-P	$ 1,802,934.00	$ 1,568,552.58
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-LS-3Y-P	$ 2,112,831.00	$ 1,838,162.97
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-LS-3Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-LS-3Y-P	$ 5,064,327.00	$ 4,405,964.49
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-LS-3Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-LS-3Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-LS-3Y-P	############	$ 8,811,928.98

FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-LS-3Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-LS-3Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-LS-4Y-P	$ 1,969,644.00	$ 1,713,590.28
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-LS-4Y-P	$ 2,403,912.00	$ 2,091,403.44
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-LS-4Y-P	$ 2,817,108.00	$ 2,450,883.96
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-LS-4Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-LS-4Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-LS-4Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-LS-4Y-P	##########	$ 9,791,032.20
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-LS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-LS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-LS-4Y-P	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-LS-1Y-PPP	$ 517,032.00	$ 449,817.84
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-LS-1Y-PPP	$ 631,027.00	$ 548,993.49
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-LS-1Y-PPP	$ 739,491.00	$ 643,357.17
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-LS-1Y-PPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-LS-1Y-PPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-LS-1Y-PPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-LS-1Y-PPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-LS-1Y-PPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-LS-1Y-PPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-LS-1Y-PPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-LS-2Y-PPP	$ 1,034,064.00	$ 899,635.68
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-LS-2Y-PPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-LS-2Y-PPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-LS-2Y-PPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-LS-2Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-LS-2Y-PPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-LS-2Y-PPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-LS-2Y-PPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-LS-2Y-PPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-LS-2Y-PPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-LS-3Y-PPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-LS-3Y-PPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-LS-3Y-PPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-LS-3Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-LS-3Y-PPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-LS-3Y-PPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-LS-3Y-PPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-LS-3Y-PPP	##########	$ 9,252,525.69
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-LS-3Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-LS-3Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-LS-4Y-PPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-LS-4Y-PPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-LS-4Y-PPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-LS-4Y-PPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-LS-4Y-PPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-LS-4Y-PPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-LS-4Y-PPP	##########	##########

FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-LS-5Y-PPP	$ 2,585,160.00	$ 2,249,089.20
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-LS-5Y-PPP	$ 3,155,135.00	$ 2,744,967.45
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-LS-5Y-PPP	$ 3,697,455.00	$ 3,216,785.85
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-LS-5Y-PPP	$ 5,908,380.00	$ 5,140,290.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-LS-5Y-PPP	$ 8,862,570.00	$ 7,710,435.90
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-LS-5Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-LS-1Y-PPP	$ 517,032.00	$ 449,817.84
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-1Y-PPP	$ 631,027.00	$ 548,993.49
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-LS-1Y-PPP	$ 739,491.00	$ 643,357.17
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-LS-1Y-PPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-LS-1Y-PPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-LS-1Y-PPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-LS-1Y-PPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-LS-1Y-PPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-LS-1Y-PPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-LS-1Y-PPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-LS-2Y-PPP	$ 1,034,064.00	$ 899,635.68
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-2Y-PPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-LS-2Y-PPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-LS-2Y-PPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-LS-2Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-LS-2Y-PPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-LS-2Y-PPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-LS-2Y-PPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-LS-2Y-PPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-LS-2Y-PPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-LS-3Y-PPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-3Y-PPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-LS-3Y-PPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-LS-3Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-LS-3Y-PPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-LS-3Y-PPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-LS-3Y-PPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-LS-3Y-PPP	##########	$ 9,252,525.69
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-LS-3Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-LS-3Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-LS-4Y-PPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-4Y-PPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-LS-4Y-PPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-LS-4Y-PPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-LS-4Y-PPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-LS-4Y-PPP	$ 9,453,412.00	$ 8,224,468.44

FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - Platinum	TAP-1KEPS-DT2SS-1Y-P-A	$ 122,185.00	$ 106,300.95
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-DT2SS-1Y-P-A	$ 157,270.00	$ 136,824.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - Platinum	TAP-5KEPS-DT2SS-1Y-P-A	$ 193,405.00	$ 168,262.35
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - Platinum	TAP-10KEPS-DT2SS-1Y-P-A	$ 327,834.00	$ 285,215.58
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - Platinum	TAP-15KEPS-DT2SS-1Y-P-A	$ 491,751.00	$ 427,823.37
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - Platinum	TAP-20KEPS-DT2SS-1Y-P-A	$ 686,854.00	$ 597,562.98
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - Platinum	TAP-25KEPS-DT2SS-1Y-P-A	$ 875,135.00	$ 761,367.45
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - Platinum	TAP-30KEPS-DT2SS-1Y-P-A	$ 1,050,162.00	$ 913,640.94
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - Platinum	TAP-35KEPS-DT2SS-1Y-P-A	$ 1,225,189.00	$ 1,065,914.43
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - Platinum	TAP-40KEPS-DT2SS-1Y-P-A	$ 1,400,216.00	$ 1,218,187.92
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - Platinum	TAP-45KEPS-DT2SS-1Y-P-A	$ 1,575,243.00	$ 1,370,461.41
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - Platinum	TAP-50KEPS-DT2SS-1Y-P-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - Platinum	TAP-55KEPS-DT2SS-1Y-P-A	$ 1,925,297.00	$ 1,675,008.39
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - Platinum	TAP-60KEPS-DT2SS-1Y-P-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - Platinum	TAP-65KEPS-DT2SS-1Y-P-A	$ 2,275,351.00	$ 1,979,555.37
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - Platinum	TAP-70KEPS-DT2SS-1Y-P-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - Platinum	TAP-75KEPS-DT2SS-1Y-P-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - Platinum	TAP-80KEPS-DT2SS-1Y-P-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - Platinum	TAP-1KEPS-DT2SS-2Y-P-A	$ 244,370.00	$ 212,601.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-DT2SS-2Y-P-A	$ 314,540.00	$ 273,649.80
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - Platinum	TAP-5KEPS-DT2SS-2Y-P-A	$ 386,810.00	$ 336,524.70
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - Platinum	TAP-10KEPS-DT2SS-2Y-P-A	$ 655,668.00	$ 570,431.16
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - Platinum	TAP-15KEPS-DT2SS-2Y-P-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - Platinum	TAP-20KEPS-DT2SS-2Y-P-A	$ 1,373,708.00	$ 1,195,125.96
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - Platinum	TAP-25KEPS-DT2SS-2Y-P-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - Platinum	TAP-30KEPS-DT2SS-2Y-P-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - Platinum	TAP-35KEPS-DT2SS-2Y-P-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - Platinum	TAP-40KEPS-DT2SS-2Y-P-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - Platinum	TAP-45KEPS-DT2SS-2Y-P-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - Platinum	TAP-50KEPS-DT2SS-2Y-P-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - Platinum	TAP-55KEPS-DT2SS-2Y-P-A	$ 3,850,594.00	$ 3,350,016.78
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - Platinum	TAP-60KEPS-DT2SS-2Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - Platinum	TAP-65KEPS-DT2SS-2Y-P-A	$ 4,550,702.00	$ 3,959,110.74
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - Platinum	TAP-70KEPS-DT2SS-2Y-P-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - Platinum	TAP-75KEPS-DT2SS-2Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - Platinum	TAP-80KEPS-DT2SS-2Y-P-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - Platinum	TAP-1KEPS-DT2SS-3Y-P-A	$ 366,555.00	$ 318,902.85
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-DT2SS-3Y-P-A	$ 471,810.00	$ 410,474.70
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - Platinum	TAP-5KEPS-DT2SS-3Y-P-A	$ 580,215.00	$ 504,787.05
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - Platinum	TAP-10KEPS-DT2SS-3Y-P-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - Platinum	TAP-15KEPS-DT2SS-3Y-P-A	$ 1,475,253.00	$ 1,283,470.11
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - Platinum	TAP-20KEPS-DT2SS-3Y-P-A	$ 2,060,562.00	$ 1,792,688.94
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - Platinum	TAP-25KEPS-DT2SS-3Y-P-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - Platinum	TAP-30KEPS-DT2SS-3Y-P-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - Platinum	TAP-35KEPS-DT2SS-3Y-P-A	$ 3,675,567.00	$ 3,197,743.29

FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - Platinum	TAP-40KEPS-DT2SS-3Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - Platinum	TAP-45KEPS-DT2SS-3Y-P-A	$ 4,725,729.00	$ 4,111,384.23
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - Platinum	TAP-50KEPS-DT2SS-3Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - Platinum	TAP-55KEPS-DT2SS-3Y-P-A	$ 5,775,891.00	$ 5,025,025.17
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - Platinum	TAP-60KEPS-DT2SS-3Y-P-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - Platinum	TAP-65KEPS-DT2SS-3Y-P-A	$ 6,826,053.00	$ 5,938,666.11
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - Platinum	TAP-70KEPS-DT2SS-3Y-P-A	$ 7,351,134.00	$ 6,395,486.58
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - Platinum	TAP-75KEPS-DT2SS-3Y-P-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - Platinum	TAP-80KEPS-DT2SS-3Y-P-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - Platinum	TAP-1KEPS-DT2SS-4Y-P-A	$ 488,740.00	$ 425,203.80
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-DT2SS-4Y-P-A	$ 629,080.00	$ 547,299.60
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - Platinum	TAP-5KEPS-DT2SS-4Y-P-A	$ 773,620.00	$ 673,049.40
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - Platinum	TAP-10KEPS-DT2SS-4Y-P-A	$ 1,311,336.00	$ 1,140,862.32
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - Platinum	TAP-15KEPS-DT2SS-4Y-P-A	$ 1,967,004.00	$ 1,711,293.48
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - Platinum	TAP-20KEPS-DT2SS-4Y-P-A	$ 2,747,416.00	$ 2,390,251.92
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - Platinum	TAP-25KEPS-DT2SS-4Y-P-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - Platinum	TAP-30KEPS-DT2SS-4Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - Platinum	TAP-35KEPS-DT2SS-4Y-P-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - Platinum	TAP-40KEPS-DT2SS-4Y-P-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - Platinum	TAP-45KEPS-DT2SS-4Y-P-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - Platinum	TAP-50KEPS-DT2SS-4Y-P-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - Platinum	TAP-55KEPS-DT2SS-4Y-P-A	$ 7,701,188.00	$ 6,700,033.56
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - Platinum	TAP-60KEPS-DT2SS-4Y-P-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - Platinum	TAP-65KEPS-DT2SS-4Y-P-A	$ 9,101,404.00	$ 7,918,221.48
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - Platinum	TAP-70KEPS-DT2SS-4Y-P-A	$ 9,801,512.00	$ 8,527,315.44
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - Platinum	TAP-75KEPS-DT2SS-4Y-P-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - Platinum	TAP-80KEPS-DT2SS-4Y-P-A	##############	$ 9,745,503.36
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - Platinum	TAP-1KEPS-DT2SS-5Y-P-A	$ 610,925.00	$ 531,504.75
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-DT2SS-5Y-P-A	$ 786,350.00	$ 684,124.50
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - Platinum	TAP-5KEPS-DT2SS-5Y-P-A	$ 967,025.00	$ 841,311.75
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - Platinum	TAP-10KEPS-DT2SS-5Y-P-A	$ 1,639,170.00	$ 1,426,077.90
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - Platinum	TAP-15KEPS-DT2SS-5Y-P-A	$ 2,458,755.00	$ 2,139,116.85
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - Platinum	TAP-20KEPS-DT2SS-5Y-P-A	$ 3,434,270.00	$ 2,987,814.90
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - Platinum	TAP-25KEPS-DT2SS-5Y-P-A	$ 4,375,675.00	$ 3,806,837.25
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - Platinum	TAP-30KEPS-DT2SS-5Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - Platinum	TAP-35KEPS-DT2SS-5Y-P-A	$ 6,125,945.00	$ 5,329,572.15
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - Platinum	TAP-40KEPS-DT2SS-5Y-P-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - Platinum	TAP-45KEPS-DT2SS-5Y-P-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - Platinum	TAP-50KEPS-DT2SS-5Y-P-A	$ 8,751,350.00	$ 7,613,674.50
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - Platinum	TAP-55KEPS-DT2SS-5Y-P-A	$ 9,626,485.00	$ 8,375,041.95
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - Platinum	TAP-60KEPS-DT2SS-5Y-P-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - Platinum	TAP-65KEPS-DT2SS-5Y-P-A	##############	$ 9,897,776.85
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - Platinum	TAP-70KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - Platinum	TAP-75KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - Platinum	TAP-80KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-DT2SS-1Y-PPP-A	$ 128,294.00	$ 111,615.78
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-1Y-PPP-	$ 165,134.00	$ 143,666.58
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-DT2SS-1Y-PPP-A	$ 203,076.00	$ 176,676.12
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-DT2SS-1Y-PPP-A	$ 344,225.00	$ 299,475.75

FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-DT2SS-1Y-PPP-A	$ 516,338.00	$ 449,214.06
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-DT2SS-1Y-PPP-A	$ 721,197.00	$ 627,441.39
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-DT2SS-1Y-PPP-A	$ 918,892.00	$ 799,436.04
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-DT2SS-1Y-PPP-A	$ 1,102,670.00	$ 959,322.90
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-DT2SS-1Y-PPP-A	$ 1,286,448.00	$ 1,119,209.76
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-DT2SS-1Y-PPP-A	$ 1,470,227.00	$ 1,279,097.49
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-DT2SS-1Y-PPP-A	$ 1,654,005.00	$ 1,438,984.35
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-DT2SS-1Y-PPP-A	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-DT2SS-1Y-PPP-A	$ 2,021,562.00	$ 1,758,758.94
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-DT2SS-1Y-PPP-A	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-DT2SS-1Y-PPP-A	$ 2,389,119.00	$ 2,078,533.53
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-DT2SS-1Y-PPP-A	$ 2,572,897.00	$ 2,238,420.39
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-DT2SS-1Y-PPP-A	$ 2,756,675.00	$ 2,398,307.25
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-DT2SS-1Y-PPP-A	$ 2,940,453.00	$ 2,558,194.11
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-DT2SS-2Y-PPP-A	$ 256,588.00	$ 223,231.56
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-2Y-PPP-	$ 330,268.00	$ 287,333.16
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-DT2SS-2Y-PPP-A	$ 406,152.00	$ 353,352.24
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-DT2SS-2Y-PPP-A	$ 688,450.00	$ 598,951.50
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-DT2SS-2Y-PPP-A	$ 1,032,676.00	$ 898,428.12
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-DT2SS-2Y-PPP-A	$ 1,442,394.00	$ 1,254,882.78
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-DT2SS-2Y-PPP-A	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-DT2SS-2Y-PPP-A	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-DT2SS-2Y-PPP-A	$ 2,572,896.00	$ 2,238,419.52
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-DT2SS-2Y-PPP-A	$ 2,940,454.00	$ 2,558,194.98
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-DT2SS-2Y-PPP-A	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-DT2SS-2Y-PPP-A	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-DT2SS-2Y-PPP-A	$ 4,043,124.00	$ 3,517,517.88
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-DT2SS-2Y-PPP-A	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-DT2SS-2Y-PPP-A	$ 4,778,238.00	$ 4,157,067.06
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-DT2SS-2Y-PPP-A	$ 5,145,794.00	$ 4,476,840.78
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-DT2SS-2Y-PPP-A	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-DT2SS-2Y-PPP-A	$ 5,880,906.00	$ 5,116,388.22
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-DT2SS-3Y-PPP-A	$ 384,882.00	$ 334,847.34
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-3Y-PPP-	$ 495,402.00	$ 430,999.74
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-DT2SS-3Y-PPP-A	$ 609,228.00	$ 530,028.36
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-DT2SS-3Y-PPP-A	$ 1,032,675.00	$ 898,427.25
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-DT2SS-3Y-PPP-A	$ 1,549,014.00	$ 1,347,642.18
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-DT2SS-3Y-PPP-A	$ 2,163,591.00	$ 1,882,324.17
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-DT2SS-3Y-PPP-A	$ 2,756,676.00	$ 2,398,308.12
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-DT2SS-3Y-PPP-A	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-DT2SS-3Y-PPP-A	$ 3,859,344.00	$ 3,357,629.28
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-DT2SS-3Y-PPP-A	$ 4,410,681.00	$ 3,837,292.47
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-DT2SS-3Y-PPP-A	$ 4,962,015.00	$ 4,316,953.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-DT2SS-3Y-PPP-A	$ 5,513,352.00	$ 4,796,616.24
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-DT2SS-3Y-PPP-A	$ 6,064,686.00	$ 5,276,276.82
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-DT2SS-3Y-PPP-A	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-DT2SS-3Y-PPP-A	$ 7,167,357.00	$ 6,235,600.59
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-DT2SS-3Y-PPP-A	$ 7,718,691.00	$ 6,715,261.17
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-DT2SS-3Y-PPP-A	$ 8,270,025.00	$ 7,194,921.75

FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-DT2SS-3Y-PPP-A	$ 8,821,359.00	$ 7,674,582.33
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-DT2SS-4Y-PPP-A	$ 513,176.00	$ 446,463.12
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-4Y-PPP-	$ 660,536.00	$ 574,666.32
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-DT2SS-4Y-PPP-A	$ 812,304.00	$ 706,704.48
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-DT2SS-4Y-PPP-A	$ 1,376,900.00	$ 1,197,903.00
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-DT2SS-4Y-PPP-A	$ 2,065,352.00	$ 1,796,856.24
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-DT2SS-4Y-PPP-A	$ 2,884,788.00	$ 2,509,765.56
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-DT2SS-4Y-PPP-A	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-DT2SS-4Y-PPP-A	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-DT2SS-4Y-PPP-A	$ 5,145,792.00	$ 4,476,839.04
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-DT2SS-4Y-PPP-A	$ 5,880,908.00	$ 5,116,389.96
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-DT2SS-4Y-PPP-A	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-DT2SS-4Y-PPP-A	$ 7,351,136.00	$ 6,395,488.32
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-DT2SS-4Y-PPP-A	$ 8,086,248.00	$ 7,035,035.76
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-DT2SS-4Y-PPP-A	$ 8,821,360.00	$ 7,674,583.20
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-DT2SS-4Y-PPP-A	$ 9,556,476.00	$ 8,314,134.12
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-DT2SS-4Y-PPP-A	##############	$ 8,953,681.56
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-DT2SS-4Y-PPP-A	##############	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-DT2SS-4Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-DT2SS-5Y-PPP-A	$ 641,470.00	$ 558,078.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-5Y-PPP-	$ 825,670.00	$ 718,332.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-DT2SS-5Y-PPP-A	$ 1,015,380.00	$ 883,380.60
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-DT2SS-5Y-PPP-A	$ 1,721,125.00	$ 1,497,378.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-DT2SS-5Y-PPP-A	$ 2,581,690.00	$ 2,246,070.30
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-DT2SS-5Y-PPP-A	$ 3,605,985.00	$ 3,137,206.95
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-DT2SS-5Y-PPP-A	$ 4,594,460.00	$ 3,997,180.20
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-DT2SS-5Y-PPP-A	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-DT2SS-5Y-PPP-A	$ 6,432,240.00	$ 5,596,048.80
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-DT2SS-5Y-PPP-A	$ 7,351,135.00	$ 6,395,487.45
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-DT2SS-5Y-PPP-A	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-DT2SS-5Y-PPP-A	$ 9,188,920.00	$ 7,994,360.40
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-DT2SS-5Y-PPP-A	##############	$ 8,793,794.70
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-DT2SS-5Y-PPP-A	##############	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-DT2SS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-DT2SS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-DT2SS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-DT2SS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-DT2LS-1Y-P-A	$ 381,961.00	$ 332,306.07
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-DT2LS-1Y-P-A	$ 481,990.00	$ 419,331.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-DT2LS-1Y-P-A	$ 583,069.00	$ 507,270.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-DT2LS-1Y-P-A	$ 977,274.00	$ 850,228.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-DT2LS-1Y-P-A	$ 1,465,911.00	$ 1,275,342.57
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-DT2LS-1Y-P-A	$ 1,985,734.00	$ 1,727,588.58
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-DT2LS-1Y-P-A	$ 2,498,735.00	$ 2,173,899.45
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-DT2LS-1Y-P-A	$ 2,998,482.00	$ 2,608,679.34
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-DT2LS-1Y-P-A	$ 3,498,229.00	$ 3,043,459.23
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-DT2LS-1Y-P-A	$ 3,997,976.00	$ 3,478,239.12
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-DT2LS-2Y-P-A	$ 763,922.00	$ 664,612.14
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-DT2LS-2Y-P-A	$ 963,980.00	$ 838,662.60

FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-DT2LS-2Y-P-A	$ 1,166,138.00	$ 1,014,540.06
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-DT2LS-2Y-P-A	$ 1,954,548.00	$ 1,700,456.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-DT2LS-2Y-P-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-DT2LS-2Y-P-A	$ 3,971,468.00	$ 3,455,177.16
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-DT2LS-2Y-P-A	$ 4,997,470.00	$ 4,347,798.90
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-DT2LS-2Y-P-A	$ 5,996,964.00	$ 5,217,358.68
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-DT2LS-2Y-P-A	$ 6,996,458.00	$ 6,086,918.46
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-DT2LS-2Y-P-A	$ 7,995,952.00	$ 6,956,478.24
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-DT2LS-3Y-P-A	$ 1,145,883.00	$ 996,918.21
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-DT2LS-3Y-P-A	$ 1,445,970.00	$ 1,257,993.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-DT2LS-3Y-P-A	$ 1,749,207.00	$ 1,521,810.09
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-DT2LS-3Y-P-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-DT2LS-3Y-P-A	$ 4,397,733.00	$ 3,826,027.71
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-DT2LS-3Y-P-A	$ 5,957,202.00	$ 5,182,765.74
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-DT2LS-3Y-P-A	$ 7,496,205.00	$ 6,521,698.35
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-DT2LS-3Y-P-A	$ 8,995,446.00	$ 7,826,038.02
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-DT2LS-3Y-P-A	##########	$ 9,130,377.69
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-DT2LS-3Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-DT2LS-4Y-P-A	$ 1,527,844.00	$ 1,329,224.28
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-DT2LS-4Y-P-A	$ 1,927,960.00	$ 1,677,325.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-DT2LS-4Y-P-A	$ 2,332,276.00	$ 2,029,080.12
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-DT2LS-4Y-P-A	$ 3,909,096.00	$ 3,400,913.52
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-DT2LS-4Y-P-A	$ 5,863,644.00	$ 5,101,370.28
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-DT2LS-4Y-P-A	$ 7,942,936.00	$ 6,910,354.32
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-DT2LS-4Y-P-A	$ 9,994,940.00	$ 8,695,597.80
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-DT2LS-5Y-P-A	$ 1,909,805.00	$ 1,661,530.35
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-DT2LS-5Y-P-A	$ 2,409,950.00	$ 2,096,656.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-DT2LS-5Y-P-A	$ 2,915,345.00	$ 2,536,350.15
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-DT2LS-5Y-P-A	$ 4,886,370.00	$ 4,251,141.90
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-DT2LS-5Y-P-A	$ 7,329,555.00	$ 6,376,712.85
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-DT2LS-5Y-P-A	$ 9,928,670.00	$ 8,637,942.90
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-DT2LS-1Y-PPP-A	$ 401,059.00	$ 348,921.33
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-1Y-PPP-A	$ 506,090.00	$ 440,298.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-DT2LS-1Y-PPP-A	$ 612,223.00	$ 532,634.01
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-DT2LS-1Y-PPP-A	$ 1,026,137.00	$ 892,739.19
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-DT2LS-1Y-PPP-A	$ 1,539,206.00	$ 1,339,109.22
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-DT2LS-1Y-PPP-A	$ 2,085,021.00	$ 1,813,968.27
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-DT2LS-1Y-PPP-A	$ 2,623,672.00	$ 2,282,594.64
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-DT2LS-1Y-PPP-A	$ 3,148,406.00	$ 2,739,113.22
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-DT2LS-1Y-PPP-A	$ 3,673,140.00	$ 3,195,631.80
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-DT2LS-1Y-PPP-A	$ 4,197,875.00	$ 3,652,151.25
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-DT2LS-2Y-PPP-A	$ 802,118.00	$ 697,842.66

FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-2Y-PPP-A	$ 1,012,180.00	$ 880,596.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-DT2LS-2Y-PPP-A	$ 1,224,446.00	$ 1,065,268.02
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-DT2LS-2Y-PPP-A	$ 2,052,274.00	$ 1,785,478.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-DT2LS-2Y-PPP-A	$ 3,078,412.00	$ 2,678,218.44
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-DT2LS-2Y-PPP-A	$ 4,170,042.00	$ 3,627,936.54
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-DT2LS-2Y-PPP-A	$ 5,247,344.00	$ 4,565,189.28
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-DT2LS-2Y-PPP-A	$ 6,296,812.00	$ 5,478,226.44
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-DT2LS-2Y-PPP-A	$ 7,346,280.00	$ 6,391,263.60
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-DT2LS-2Y-PPP-A	$ 8,395,750.00	$ 7,304,302.50
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-DT2LS-3Y-PPP-A	$ 1,203,177.00	$ 1,046,763.99
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-3Y-PPP-A	$ 1,518,270.00	$ 1,320,894.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-DT2LS-3Y-PPP-A	$ 1,836,669.00	$ 1,597,902.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-DT2LS-3Y-PPP-A	$ 3,078,411.00	$ 2,678,217.57
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-DT2LS-3Y-PPP-A	$ 4,617,618.00	$ 4,017,327.66
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-DT2LS-3Y-PPP-A	$ 6,255,063.00	$ 5,441,904.81
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-DT2LS-3Y-PPP-A	$ 7,871,016.00	$ 6,847,783.92
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-DT2LS-3Y-PPP-A	$ 9,445,218.00	$ 8,217,339.66
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-DT2LS-3Y-PPP-A	##############	$ 9,586,895.40
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-DT2LS-3Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-DT2LS-4Y-PPP-A	$ 1,604,236.00	$ 1,395,685.32
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-4Y-PPP-A	$ 2,024,360.00	$ 1,761,193.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-DT2LS-4Y-PPP-A	$ 2,448,892.00	$ 2,130,536.04
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-DT2LS-4Y-PPP-A	$ 4,104,548.00	$ 3,570,956.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-DT2LS-4Y-PPP-A	$ 6,156,824.00	$ 5,356,436.88
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-DT2LS-4Y-PPP-A	$ 8,340,084.00	$ 7,255,873.08
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-DT2LS-4Y-PPP-A	##############	$ 9,130,378.56
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-DT2LS-4Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-DT2LS-4Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-DT2LS-4Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-DT2LS-5Y-PPP-A	$ 2,005,295.00	$ 1,744,606.65
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-5Y-PPP-A	$ 2,530,450.00	$ 2,201,491.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-DT2LS-5Y-PPP-A	$ 3,061,115.00	$ 2,663,170.05
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-DT2LS-5Y-PPP-A	$ 5,130,685.00	$ 4,463,695.95
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-DT2LS-5Y-PPP-A	$ 7,696,030.00	$ 6,695,546.10
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-DT2LS-5Y-PPP-A	##############	$ 9,069,841.35
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-DT2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-DT2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-DT2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-DT2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-SS2LS-1Y-P-A	$ 259,776.00	$ 226,005.12
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-SS2LS-1Y-P-A	$ 324,720.00	$ 282,506.40
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-SS2LS-1Y-P-A	$ 389,664.00	$ 339,007.68
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-SS2LS-1Y-P-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-SS2LS-1Y-P-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-SS2LS-1Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-SS2LS-1Y-P-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-SS2LS-1Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-SS2LS-1Y-P-A	$ 2,273,040.00	$ 1,977,544.80
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-SS2LS-1Y-P-A	$ 2,597,760.00	$ 2,260,051.20

FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-SS2LS-2Y-P-A	$ 519,552.00	$ 452,010.24
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-SS2LS-2Y-P-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-SS2LS-2Y-P-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-SS2LS-2Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-SS2LS-2Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-SS2LS-2Y-P-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-SS2LS-2Y-P-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-SS2LS-2Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-SS2LS-2Y-P-A	$ 4,546,080.00	$ 3,955,089.60
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-SS2LS-2Y-P-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-SS2LS-3Y-P-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-SS2LS-3Y-P-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-SS2LS-3Y-P-A	$ 1,168,992.00	$ 1,017,023.04
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-SS2LS-3Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-SS2LS-3Y-P-A	$ 2,922,480.00	$ 2,542,557.60
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-SS2LS-3Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-SS2LS-3Y-P-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-SS2LS-3Y-P-A	$ 5,844,960.00	$ 5,085,115.20
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-SS2LS-3Y-P-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-SS2LS-3Y-P-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-SS2LS-4Y-P-A	$ 1,039,104.00	$ 904,020.48
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-SS2LS-4Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-SS2LS-4Y-P-A	$ 1,558,656.00	$ 1,356,030.72
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-SS2LS-4Y-P-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-SS2LS-4Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-SS2LS-4Y-P-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-SS2LS-4Y-P-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-SS2LS-4Y-P-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-SS2LS-4Y-P-A	$ 9,092,160.00	$ 7,910,179.20
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-SS2LS-4Y-P-A	##############	$ 9,040,204.80
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-SS2LS-5Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-SS2LS-5Y-P-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-SS2LS-5Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-SS2LS-5Y-P-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-SS2LS-5Y-P-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-SS2LS-5Y-P-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-SS2LS-5Y-P-A	$ 8,118,000.00	$ 7,062,660.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-SS2LS-5Y-P-A	$ 9,741,600.00	$ 8,475,192.00
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-SS2LS-5Y-P-A	##############	$ 9,887,724.00
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-SS2LS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-SS2LS-1Y-PPP-A	$ 272,765.00	$ 237,305.55
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-1Y-PPP-A	$ 340,956.00	$ 296,631.72
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-SS2LS-1Y-PPP-A	$ 409,147.00	$ 355,957.89
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-SS2LS-1Y-PPP-A	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-SS2LS-1Y-PPP-A	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-SS2LS-1Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-SS2LS-1Y-PPP-A	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-SS2LS-1Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-SS2LS-1Y-PPP-A	$ 2,386,692.00	$ 2,076,422.04

FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-SS2LS-1Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-SS2LS-2Y-PPP-A	$ 545,530.00	$ 474,611.10
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-2Y-PPP-A	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-SS2LS-2Y-PPP-A	$ 818,294.00	$ 711,915.78
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-SS2LS-2Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-SS2LS-2Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-SS2LS-2Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-SS2LS-2Y-PPP-A	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-SS2LS-2Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-SS2LS-2Y-PPP-A	$ 4,773,384.00	$ 4,152,844.08
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-SS2LS-2Y-PPP-A	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-SS2LS-3Y-PPP-A	$ 818,295.00	$ 711,916.65
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-3Y-PPP-A	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-SS2LS-3Y-PPP-A	$ 1,227,441.00	$ 1,067,873.67
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-SS2LS-3Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-SS2LS-3Y-PPP-A	$ 3,068,604.00	$ 2,669,685.48
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-SS2LS-3Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-SS2LS-3Y-PPP-A	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-SS2LS-3Y-PPP-A	$ 6,137,208.00	$ 5,339,370.96
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-SS2LS-3Y-PPP-A	$ 7,160,076.00	$ 6,229,266.12
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-SS2LS-3Y-PPP-A	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-SS2LS-4Y-PPP-A	$ 1,091,060.00	$ 949,222.20
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-4Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-SS2LS-4Y-PPP-A	$ 1,636,588.00	$ 1,423,831.56
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-SS2LS-4Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-SS2LS-4Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-SS2LS-4Y-PPP-A	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-SS2LS-4Y-PPP-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-SS2LS-4Y-PPP-A	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-SS2LS-4Y-PPP-A	$ 9,546,768.00	$ 8,305,688.16
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-SS2LS-4Y-PPP-A	##############	$ 9,492,215.04
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-SS2LS-5Y-PPP-A	$ 1,363,825.00	$ 1,186,527.75
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-5Y-PPP-A	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-SS2LS-5Y-PPP-A	$ 2,045,735.00	$ 1,779,789.45
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-SS2LS-5Y-PPP-A	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-SS2LS-5Y-PPP-A	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-SS2LS-5Y-PPP-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-SS2LS-5Y-PPP-A	$ 8,523,900.00	$ 7,415,793.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-SS2LS-5Y-PPP-A	##############	$ 8,898,951.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-SS2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-SS2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS	TAP-1KEPS-BD-1Y-US	$ 110,450.00	$ 96,091.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-BD-1Y-US	$ 118,988.00	$ 103,519.56
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS	TAP-5KEPS-BD-1Y-US	$ 121,208.00	$ 105,450.96
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS	TAP-10KEPS-BD-1Y-US	$ 148,132.00	$ 128,874.84
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS	TAP-15KEPS-BD-1Y-US	$ 222,198.00	$ 193,312.26
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS	TAP-20KEPS-BD-1Y-US	$ 265,078.00	$ 230,617.86
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS	TAP-25KEPS-BD-1Y-US	$ 314,780.00	$ 273,858.60
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS	TAP-30KEPS-BD-1Y-US	$ 377,736.00	$ 328,630.32

FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS	TAP-35KEPS-BD-1Y-US	$ 440,692.00	$ 383,402.04
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS	TAP-40KEPS-BD-1Y-US	$ 503,648.00	$ 438,173.76
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS	TAP-45KEPS-BD-1Y-US	$ 566,604.00	$ 492,945.48
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS	TAP-50KEPS-BD-1Y-US	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS	TAP-55KEPS-BD-1Y-US	$ 692,516.00	$ 602,488.92
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS	TAP-60KEPS-BD-1Y-US	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS	TAP-65KEPS-BD-1Y-US	$ 818,428.00	$ 712,032.36
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS	TAP-70KEPS-BD-1Y-US	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS	TAP-75KEPS-BD-1Y-US	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS	TAP-80KEPS-BD-1Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS	TAP-1KEPS-BD-2Y-US	$ 220,900.00	$ 192,183.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-BD-2Y-US	$ 237,976.00	$ 207,039.12
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS	TAP-5KEPS-BD-2Y-US	$ 242,416.00	$ 210,901.92
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS	TAP-10KEPS-BD-2Y-US	$ 296,264.00	$ 257,749.68
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS	TAP-15KEPS-BD-2Y-US	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS	TAP-20KEPS-BD-2Y-US	$ 530,156.00	$ 461,235.72
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS	TAP-25KEPS-BD-2Y-US	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS	TAP-30KEPS-BD-2Y-US	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS	TAP-35KEPS-BD-2Y-US	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS	TAP-40KEPS-BD-2Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS	TAP-45KEPS-BD-2Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS	TAP-50KEPS-BD-2Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS	TAP-55KEPS-BD-2Y-US	$ 1,385,032.00	$ 1,204,977.84
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS	TAP-60KEPS-BD-2Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS	TAP-65KEPS-BD-2Y-US	$ 1,636,856.00	$ 1,424,064.72
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS	TAP-70KEPS-BD-2Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS	TAP-75KEPS-BD-2Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS	TAP-80KEPS-BD-2Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS	TAP-1KEPS-BD-3Y-US	$ 331,350.00	$ 288,274.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-BD-3Y-US	$ 356,964.00	$ 310,558.68
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS	TAP-5KEPS-BD-3Y-US	$ 363,624.00	$ 316,352.88
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS	TAP-10KEPS-BD-3Y-US	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS	TAP-15KEPS-BD-3Y-US	$ 666,594.00	$ 579,936.78
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS	TAP-20KEPS-BD-3Y-US	$ 795,234.00	$ 691,853.58
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS	TAP-25KEPS-BD-3Y-US	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS	TAP-30KEPS-BD-3Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS	TAP-35KEPS-BD-3Y-US	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS	TAP-40KEPS-BD-3Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS	TAP-45KEPS-BD-3Y-US	$ 1,699,812.00	$ 1,478,836.44
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS	TAP-50KEPS-BD-3Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS	TAP-55KEPS-BD-3Y-US	$ 2,077,548.00	$ 1,807,466.76
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS	TAP-60KEPS-BD-3Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS	TAP-65KEPS-BD-3Y-US	$ 2,455,284.00	$ 2,136,097.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS	TAP-70KEPS-BD-3Y-US	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS	TAP-75KEPS-BD-3Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS	TAP-80KEPS-BD-3Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS	TAP-1KEPS-BD-4Y-US	$ 441,800.00	$ 384,366.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-BD-4Y-US	$ 475,952.00	$ 414,078.24
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS	TAP-5KEPS-BD-4Y-US	$ 484,832.00	$ 421,803.84

FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS	TAP-10KEPS-BD-4Y-US	$ 592,528.00	$ 515,499.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS	TAP-15KEPS-BD-4Y-US	$ 888,792.00	$ 773,249.04
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS	TAP-20KEPS-BD-4Y-US	$ 1,060,312.00	$ 922,471.44
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS	TAP-25KEPS-BD-4Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS	TAP-30KEPS-BD-4Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS	TAP-35KEPS-BD-4Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS	TAP-40KEPS-BD-4Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS	TAP-45KEPS-BD-4Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS	TAP-50KEPS-BD-4Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS	TAP-55KEPS-BD-4Y-US	$ 2,770,064.00	$ 2,409,955.68
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS	TAP-60KEPS-BD-4Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS	TAP-65KEPS-BD-4Y-US	$ 3,273,712.00	$ 2,848,129.44
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS	TAP-70KEPS-BD-4Y-US	$ 3,525,536.00	$ 3,067,216.32
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS	TAP-75KEPS-BD-4Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS	TAP-80KEPS-BD-4Y-US	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS	TAP-1KEPS-BD-5Y-US	$ 552,250.00	$ 480,457.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-BD-5Y-US	$ 594,940.00	$ 517,597.80
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS	TAP-5KEPS-BD-5Y-US	$ 606,040.00	$ 527,254.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS	TAP-10KEPS-BD-5Y-US	$ 740,660.00	$ 644,374.20
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS	TAP-15KEPS-BD-5Y-US	$ 1,110,990.00	$ 966,561.30
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS	TAP-20KEPS-BD-5Y-US	$ 1,325,390.00	$ 1,153,089.30
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS	TAP-25KEPS-BD-5Y-US	$ 1,573,900.00	$ 1,369,293.00
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS	TAP-30KEPS-BD-5Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS	TAP-35KEPS-BD-5Y-US	$ 2,203,460.00	$ 1,917,010.20
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS	TAP-40KEPS-BD-5Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS	TAP-45KEPS-BD-5Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS	TAP-50KEPS-BD-5Y-US	$ 3,147,800.00	$ 2,738,586.00
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS	TAP-55KEPS-BD-5Y-US	$ 3,462,580.00	$ 3,012,444.60
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS	TAP-60KEPS-BD-5Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS	TAP-65KEPS-BD-5Y-US	$ 4,092,140.00	$ 3,560,161.80
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS	TAP-70KEPS-BD-5Y-US	$ 4,406,920.00	$ 3,834,020.40
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS	TAP-75KEPS-BD-5Y-US	$ 4,721,700.00	$ 4,107,879.00
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS	TAP-80KEPS-BD-5Y-US	$ 5,036,480.00	$ 4,381,737.60
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-BD-1Y-US	$ 110,450.00	$ 96,091.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-BD-1Y-US	$ 118,988.00	$ 103,519.56
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-BD-1Y-US	$ 121,208.00	$ 105,450.96
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-BD-1Y-US	$ 148,132.00	$ 128,874.84
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-BD-1Y-US	$ 222,198.00	$ 193,312.26
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-BD-1Y-US	$ 265,078.00	$ 230,617.86
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-BD-1Y-US	$ 314,780.00	$ 273,858.60
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-BD-1Y-US	$ 377,736.00	$ 328,630.32
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-BD-1Y-US	$ 440,692.00	$ 383,402.04
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-BD-1Y-US	$ 503,648.00	$ 438,173.76
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS	RN-TAP-45KEPS-BD-1Y-US	$ 566,604.00	$ 492,945.48
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS	RN-TAP-50KEPS-BD-1Y-US	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS	RN-TAP-55KEPS-BD-1Y-US	$ 692,516.00	$ 602,488.92
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS	RN-TAP-60KEPS-BD-1Y-US	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS	RN-TAP-65KEPS-BD-1Y-US	$ 818,428.00	$ 712,032.36
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS	RN-TAP-70KEPS-BD-1Y-US	$ 881,384.00	$ 766,804.08

FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS	RN-TAP-75KEPS-BD-1Y-US	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS	RN-TAP-80KEPS-BD-1Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-BD-2Y-US	$ 220,900.00	$ 192,183.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-BD-2Y-US	$ 237,976.00	$ 207,039.12
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-BD-2Y-US	$ 242,416.00	$ 210,901.92
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-BD-2Y-US	$ 296,264.00	$ 257,749.68
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-BD-2Y-US	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-BD-2Y-US	$ 530,156.00	$ 461,235.72
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-BD-2Y-US	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-BD-2Y-US	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-BD-2Y-US	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-BD-2Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS	RN-TAP-45KEPS-BD-2Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS	RN-TAP-50KEPS-BD-2Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS	RN-TAP-55KEPS-BD-2Y-US	$ 1,385,032.00	$ 1,204,977.84
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS	RN-TAP-60KEPS-BD-2Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS	RN-TAP-65KEPS-BD-2Y-US	$ 1,636,856.00	$ 1,424,064.72
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS	RN-TAP-70KEPS-BD-2Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS	RN-TAP-75KEPS-BD-2Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS	RN-TAP-80KEPS-BD-2Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-BD-3Y-US	$ 331,350.00	$ 288,274.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-BD-3Y-US	$ 356,964.00	$ 310,558.68
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-BD-3Y-US	$ 363,624.00	$ 316,352.88
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-BD-3Y-US	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-BD-3Y-US	$ 666,594.00	$ 579,936.78
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-BD-3Y-US	$ 795,234.00	$ 691,853.58
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-BD-3Y-US	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-BD-3Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-BD-3Y-US	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-BD-3Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS	RN-TAP-45KEPS-BD-3Y-US	$ 1,699,812.00	$ 1,478,836.44
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS	RN-TAP-50KEPS-BD-3Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS	RN-TAP-55KEPS-BD-3Y-US	$ 2,077,548.00	$ 1,807,466.76
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS	RN-TAP-60KEPS-BD-3Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS	RN-TAP-65KEPS-BD-3Y-US	$ 2,455,284.00	$ 2,136,097.08
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS	RN-TAP-70KEPS-BD-3Y-US	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS	RN-TAP-75KEPS-BD-3Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS	RN-TAP-80KEPS-BD-3Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-BD-4Y-US	$ 441,800.00	$ 384,366.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-BD-4Y-US	$ 475,952.00	$ 414,078.24
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-BD-4Y-US	$ 484,832.00	$ 421,803.84
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-BD-4Y-US	$ 592,528.00	$ 515,499.36
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-BD-4Y-US	$ 888,792.00	$ 773,249.04
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-BD-4Y-US	$ 1,060,312.00	$ 922,471.44
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-BD-4Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-BD-4Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-BD-4Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-BD-4Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS	RN-TAP-45KEPS-BD-4Y-US	$ 2,266,416.00	$ 1,971,781.92

FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS	RN-TAP-50KEPS-BD-4Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS	RN-TAP-55KEPS-BD-4Y-US	$ 2,770,064.00	$ 2,409,955.68
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS	RN-TAP-60KEPS-BD-4Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS	RN-TAP-65KEPS-BD-4Y-US	$ 3,273,712.00	$ 2,848,129.44
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS	RN-TAP-70KEPS-BD-4Y-US	$ 3,525,536.00	$ 3,067,216.32
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS	RN-TAP-75KEPS-BD-4Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS	RN-TAP-80KEPS-BD-4Y-US	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-BD-1Y-USPP	$ 115,973.00	$ 100,896.51
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-BD-1Y-USPP	$ 124,937.00	$ 108,695.19
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-BD-1Y-USPP	$ 127,268.00	$ 110,723.16
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-BD-1Y-USPP	$ 155,539.00	$ 135,318.93
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-BD-1Y-USPP	$ 233,308.00	$ 202,977.96
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-BD-1Y-USPP	$ 278,332.00	$ 242,148.84
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-BD-1Y-USPP	$ 330,519.00	$ 287,551.53
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-BD-1Y-USPP	$ 396,623.00	$ 345,062.01
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-BD-1Y-USPP	$ 462,727.00	$ 402,572.49
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-BD-1Y-USPP	$ 528,830.00	$ 460,082.10
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-BD-1Y-USPP	$ 594,934.00	$ 517,592.58
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-BD-1Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-BD-1Y-USPP	$ 727,142.00	$ 632,613.54
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-BD-1Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-BD-1Y-USPP	$ 859,349.00	$ 747,633.63
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-BD-1Y-USPP	$ 925,453.00	$ 805,144.11
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-BD-1Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-BD-1Y-USPP	$ 1,057,661.00	$ 920,165.07
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-BD-2Y-USPP	$ 231,946.00	$ 201,793.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-BD-2Y-USPP	$ 249,874.00	$ 217,390.38
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-BD-2Y-USPP	$ 254,536.00	$ 221,446.32
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-BD-2Y-USPP	$ 311,078.00	$ 270,637.86
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-BD-2Y-USPP	$ 466,616.00	$ 405,955.92
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-BD-2Y-USPP	$ 556,664.00	$ 484,297.68
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-BD-2Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-BD-2Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-BD-2Y-USPP	$ 925,454.00	$ 805,144.98
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-BD-2Y-USPP	$ 1,057,660.00	$ 920,164.20
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-BD-2Y-USPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-BD-2Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-BD-2Y-USPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-BD-2Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-BD-2Y-USPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-BD-2Y-USPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-BD-2Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-BD-2Y-USPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-BD-3Y-USPP	$ 347,919.00	$ 302,689.53
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-BD-3Y-USPP	$ 374,811.00	$ 326,085.57
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-BD-3Y-USPP	$ 381,804.00	$ 332,169.48
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-BD-3Y-USPP	$ 466,617.00	$ 405,956.79
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-BD-3Y-USPP	$ 699,924.00	$ 608,933.88
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-BD-3Y-USPP	$ 834,996.00	$ 726,446.52

FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-BD-3Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-BD-3Y-USPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-BD-3Y-USPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-BD-3Y-USPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-BD-3Y-USPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-BD-3Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-BD-3Y-USPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-BD-3Y-USPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-BD-3Y-USPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-BD-3Y-USPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-BD-3Y-USPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-BD-3Y-USPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-BD-4Y-USPP	$ 463,892.00	$ 403,586.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-BD-4Y-USPP	$ 499,748.00	$ 434,780.76
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-BD-4Y-USPP	$ 509,072.00	$ 442,892.64
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-BD-4Y-USPP	$ 622,156.00	$ 541,275.72
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-BD-4Y-USPP	$ 933,232.00	$ 811,911.84
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-BD-4Y-USPP	$ 1,113,328.00	$ 968,595.36
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-BD-4Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-BD-4Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-BD-4Y-USPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-BD-4Y-USPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-BD-4Y-USPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-BD-4Y-USPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-BD-4Y-USPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-BD-4Y-USPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-BD-4Y-USPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-BD-4Y-USPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-BD-4Y-USPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-BD-4Y-USPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-BD-5Y-USPP	$ 579,865.00	$ 504,482.55
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-BD-5Y-USPP	$ 624,685.00	$ 543,475.95
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-BD-5Y-USPP	$ 636,340.00	$ 553,615.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-BD-5Y-USPP	$ 777,695.00	$ 676,594.65
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-BD-5Y-USPP	$ 1,166,540.00	$ 1,014,889.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-BD-5Y-USPP	$ 1,391,660.00	$ 1,210,744.20
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-BD-5Y-USPP	$ 1,652,595.00	$ 1,437,757.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-BD-5Y-USPP	$ 1,983,115.00	$ 1,725,310.05
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-BD-5Y-USPP	$ 2,313,635.00	$ 2,012,862.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-BD-5Y-USPP	$ 2,644,150.00	$ 2,300,410.50
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-BD-5Y-USPP	$ 2,974,670.00	$ 2,587,962.90
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-BD-5Y-USPP	$ 3,305,190.00	$ 2,875,515.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-BD-5Y-USPP	$ 3,635,710.00	$ 3,163,067.70
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-BD-5Y-USPP	$ 3,966,230.00	$ 3,450,620.10
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-BD-5Y-USPP	$ 4,296,745.00	$ 3,738,168.15
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-BD-5Y-USPP	$ 4,627,265.00	$ 4,025,720.55
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-BD-5Y-USPP	$ 4,957,785.00	$ 4,313,272.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-BD-5Y-USPP	$ 5,288,305.00	$ 4,600,825.35
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-1Y-USPP	$ 115,973.00	$ 100,896.51

FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-1Y-USPP	$ 124,937.00	$ 108,695.19
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-1Y-USPP	$ 127,268.00	$ 110,723.16
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-1Y-USPP	$ 155,539.00	$ 135,318.93
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-1Y-USPP	$ 233,308.00	$ 202,977.96
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-1Y-USPP	$ 278,332.00	$ 242,148.84
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-1Y-USPP	$ 330,519.00	$ 287,551.53
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-1Y-USPP	$ 396,623.00	$ 345,062.01
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-1Y-USPP	$ 462,727.00	$ 402,572.49
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-1Y-USPP	$ 528,830.00	$ 460,082.10
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-1Y-USPP	$ 594,934.00	$ 517,592.58
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-1Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-1Y-USPP	$ 727,142.00	$ 632,613.54
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-1Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-1Y-USPP	$ 859,349.00	$ 747,633.63
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-1Y-USPP	$ 925,453.00	$ 805,144.11
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-1Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-1Y-USPP	$ 1,057,661.00	$ 920,165.07
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-2Y-USPP	$ 231,946.00	$ 201,793.02
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-2Y-USPP	$ 249,874.00	$ 217,390.38
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-2Y-USPP	$ 254,536.00	$ 221,446.32
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-2Y-USPP	$ 311,078.00	$ 270,637.86
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-2Y-USPP	$ 466,616.00	$ 405,955.92
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-2Y-USPP	$ 556,664.00	$ 484,297.68
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-2Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-2Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-2Y-USPP	$ 925,454.00	$ 805,144.98
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-2Y-USPP	$ 1,057,660.00	$ 920,164.20
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-2Y-USPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-2Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-2Y-USPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-2Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-2Y-USPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-2Y-USPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-2Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-2Y-USPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-3Y-USPP	$ 347,919.00	$ 302,689.53
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-3Y-USPP	$ 374,811.00	$ 326,085.57
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-3Y-USPP	$ 381,804.00	$ 332,169.48
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-3Y-USPP	$ 466,617.00	$ 405,956.79
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-3Y-USPP	$ 699,924.00	$ 608,933.88
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-3Y-USPP	$ 834,996.00	$ 726,446.52
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-3Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-3Y-USPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-3Y-USPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-3Y-USPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-3Y-USPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-3Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-3Y-USPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-3Y-USPP	$ 2,379,738.00	$ 2,070,372.06

FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-3Y-USPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-3Y-USPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-3Y-USPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-3Y-USPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-4Y-USPP	$ 463,892.00	$ 403,586.04
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-4Y-USPP	$ 499,748.00	$ 434,780.76
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-4Y-USPP	$ 509,072.00	$ 442,892.64
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-4Y-USPP	$ 622,156.00	$ 541,275.72
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-4Y-USPP	$ 933,232.00	$ 811,911.84
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-4Y-USPP	$ 1,113,328.00	$ 968,595.36
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-4Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-4Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-4Y-USPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-4Y-USPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-4Y-USPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-4Y-USPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-4Y-USPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-4Y-USPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-4Y-USPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-4Y-USPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-4Y-USPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-4Y-USPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS	TAP-1KEPS-SS-1Y-US	$ 232,635.00	$ 202,392.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-SS-1Y-US	$ 276,258.00	$ 240,344.46
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS	TAP-5KEPS-SS-1Y-US	$ 314,613.00	$ 273,713.31
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS	TAP-10KEPS-SS-1Y-US	$ 475,966.00	$ 414,090.42
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS	TAP-15KEPS-SS-1Y-US	$ 713,949.00	$ 621,135.63
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS	TAP-20KEPS-SS-1Y-US	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS	TAP-25KEPS-SS-1Y-US	$ 1,189,915.00	$ 1,035,226.05
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS	TAP-30KEPS-SS-1Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS	TAP-35KEPS-SS-1Y-US	$ 1,665,881.00	$ 1,449,316.47
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS	TAP-40KEPS-SS-1Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS	TAP-45KEPS-SS-1Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS	TAP-50KEPS-SS-1Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS	TAP-55KEPS-SS-1Y-US	$ 2,617,813.00	$ 2,277,497.31
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS	TAP-60KEPS-SS-1Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS	TAP-65KEPS-SS-1Y-US	$ 3,093,779.00	$ 2,691,587.73
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS	TAP-70KEPS-SS-1Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS	TAP-75KEPS-SS-1Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS	TAP-80KEPS-SS-1Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS	TAP-1KEPS-SS-2Y-US	$ 465,270.00	$ 404,784.90
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-SS-2Y-US	$ 552,516.00	$ 480,688.92
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS	TAP-5KEPS-SS-2Y-US	$ 629,226.00	$ 547,426.62
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS	TAP-10KEPS-SS-2Y-US	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS	TAP-15KEPS-SS-2Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS	TAP-20KEPS-SS-2Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS	TAP-25KEPS-SS-2Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS	TAP-30KEPS-SS-2Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS	TAP-35KEPS-SS-2Y-US	$ 3,331,762.00	$ 2,898,632.94

FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS	TAP-40KEPS-SS-2Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS	TAP-45KEPS-SS-2Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS	TAP-50KEPS-SS-2Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS	TAP-55KEPS-SS-2Y-US	$ 5,235,626.00	$ 4,554,994.62
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS	TAP-60KEPS-SS-2Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS	TAP-65KEPS-SS-2Y-US	$ 6,187,558.00	$ 5,383,175.46
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS	TAP-70KEPS-SS-2Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS	TAP-75KEPS-SS-2Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS	TAP-80KEPS-SS-2Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS	TAP-1KEPS-SS-3Y-US	$ 697,905.00	$ 607,177.35
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-SS-3Y-US	$ 828,774.00	$ 721,033.38
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS	TAP-5KEPS-SS-3Y-US	$ 943,839.00	$ 821,139.93
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS	TAP-10KEPS-SS-3Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS	TAP-15KEPS-SS-3Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS	TAP-20KEPS-SS-3Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS	TAP-25KEPS-SS-3Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS	TAP-30KEPS-SS-3Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS	TAP-35KEPS-SS-3Y-US	$ 4,997,643.00	$ 4,347,949.41
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS	TAP-40KEPS-SS-3Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS	TAP-45KEPS-SS-3Y-US	$ 6,425,541.00	$ 5,590,220.67
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS	TAP-50KEPS-SS-3Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS	TAP-55KEPS-SS-3Y-US	$ 7,853,439.00	$ 6,832,491.93
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS	TAP-60KEPS-SS-3Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS	TAP-65KEPS-SS-3Y-US	$ 9,281,337.00	$ 8,074,763.19
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS	TAP-70KEPS-SS-3Y-US	$ 9,995,286.00	$ 8,695,898.82
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS	TAP-75KEPS-SS-3Y-US	##############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS	TAP-80KEPS-SS-3Y-US	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS	TAP-1KEPS-SS-4Y-US	$ 930,540.00	$ 809,569.80
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-SS-4Y-US	$ 1,105,032.00	$ 961,377.84
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS	TAP-5KEPS-SS-4Y-US	$ 1,258,452.00	$ 1,094,853.24
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS	TAP-10KEPS-SS-4Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS	TAP-15KEPS-SS-4Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS	TAP-20KEPS-SS-4Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS	TAP-25KEPS-SS-4Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS	TAP-30KEPS-SS-4Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS	TAP-35KEPS-SS-4Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS	TAP-40KEPS-SS-4Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS	TAP-45KEPS-SS-4Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS	TAP-50KEPS-SS-4Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS	TAP-55KEPS-SS-4Y-US	##############	$ 9,109,989.24
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS	TAP-60KEPS-SS-4Y-US	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS	TAP-65KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS	TAP-70KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS	TAP-75KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS	TAP-80KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS	TAP-1KEPS-SS-5Y-US	$ 1,163,175.00	$ 1,011,962.25
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-SS-5Y-US	$ 1,381,290.00	$ 1,201,722.30
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS	TAP-5KEPS-SS-5Y-US	$ 1,573,065.00	$ 1,368,566.55
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS	TAP-10KEPS-SS-5Y-US	$ 2,379,830.00	$ 2,070,452.10

FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS	TAP-15KEPS-SS-5Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS	TAP-20KEPS-SS-5Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS	TAP-25KEPS-SS-5Y-US	$ 5,949,575.00	$ 5,176,130.25
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS	TAP-30KEPS-SS-5Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS	TAP-35KEPS-SS-5Y-US	$ 8,329,405.00	$ 7,246,582.35
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS	TAP-40KEPS-SS-5Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS	TAP-45KEPS-SS-5Y-US	############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS	TAP-50KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS	TAP-55KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS	TAP-60KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS	TAP-65KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS	TAP-70KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS	TAP-75KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS	TAP-80KEPS-SS-5Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-SS-1Y-US	$ 232,635.00	$ 202,392.45
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-SS-1Y-US	$ 276,258.00	$ 240,344.46
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-SS-1Y-US	$ 314,613.00	$ 273,713.31
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-SS-1Y-US	$ 475,966.00	$ 414,090.42
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-SS-1Y-US	$ 713,949.00	$ 621,135.63
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-SS-1Y-US	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-SS-1Y-US	$ 1,189,915.00	$ 1,035,226.05
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-SS-1Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-SS-1Y-US	$ 1,665,881.00	$ 1,449,316.47
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-SS-1Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS	RN-TAP-45KEPS-SS-1Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS	RN-TAP-50KEPS-SS-1Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS	RN-TAP-55KEPS-SS-1Y-US	$ 2,617,813.00	$ 2,277,497.31
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS	RN-TAP-60KEPS-SS-1Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS	RN-TAP-65KEPS-SS-1Y-US	$ 3,093,779.00	$ 2,691,587.73
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS	RN-TAP-70KEPS-SS-1Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS	RN-TAP-75KEPS-SS-1Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS	RN-TAP-80KEPS-SS-1Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-SS-2Y-US	$ 465,270.00	$ 404,784.90
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-SS-2Y-US	$ 552,516.00	$ 480,688.92
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-SS-2Y-US	$ 629,226.00	$ 547,426.62
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-SS-2Y-US	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-SS-2Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-SS-2Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-SS-2Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-SS-2Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-SS-2Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-SS-2Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS	RN-TAP-45KEPS-SS-2Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS	RN-TAP-50KEPS-SS-2Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS	RN-TAP-55KEPS-SS-2Y-US	$ 5,235,626.00	$ 4,554,994.62
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS	RN-TAP-60KEPS-SS-2Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS	RN-TAP-65KEPS-SS-2Y-US	$ 6,187,558.00	$ 5,383,175.46
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS	RN-TAP-70KEPS-SS-2Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS	RN-TAP-75KEPS-SS-2Y-US	$ 7,139,490.00	$ 6,211,356.30

FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS	RN-TAP-80KEPS-SS-2Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-SS-3Y-US	$ 697,905.00	$ 607,177.35
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-SS-3Y-US	$ 828,774.00	$ 721,033.38
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-SS-3Y-US	$ 943,839.00	$ 821,139.93
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-SS-3Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-SS-3Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-SS-3Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-SS-3Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-SS-3Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-SS-3Y-US	$ 4,997,643.00	$ 4,347,949.41
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-SS-3Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS	RN-TAP-45KEPS-SS-3Y-US	$ 6,425,541.00	$ 5,590,220.67
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS	RN-TAP-50KEPS-SS-3Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS	RN-TAP-55KEPS-SS-3Y-US	$ 7,853,439.00	$ 6,832,491.93
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS	RN-TAP-60KEPS-SS-3Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS	RN-TAP-65KEPS-SS-3Y-US	$ 9,281,337.00	$ 8,074,763.19
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS	RN-TAP-70KEPS-SS-3Y-US	$ 9,995,286.00	$ 8,695,898.82
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS	RN-TAP-75KEPS-SS-3Y-US	##############	$ 9,317,034.45
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS	RN-TAP-80KEPS-SS-3Y-US	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-SS-4Y-US	$ 930,540.00	$ 809,569.80
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-SS-4Y-US	$ 1,105,032.00	$ 961,377.84
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-SS-4Y-US	$ 1,258,452.00	$ 1,094,853.24
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-SS-4Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-SS-4Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-SS-4Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-SS-4Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-SS-4Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-SS-4Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-SS-4Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS	RN-TAP-45KEPS-SS-4Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS	RN-TAP-50KEPS-SS-4Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS	RN-TAP-55KEPS-SS-4Y-US	##############	$ 9,109,989.24
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS	RN-TAP-60KEPS-SS-4Y-US	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS	RN-TAP-65KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS	RN-TAP-70KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS	RN-TAP-75KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS	RN-TAP-80KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-SS-1Y-USPP	$ 244,267.00	$ 212,512.29
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-SS-1Y-USPP	$ 290,071.00	$ 252,361.77
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-SS-1Y-USPP	$ 330,344.00	$ 287,399.28
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-SS-1Y-USPP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-SS-1Y-USPP	$ 749,646.00	$ 652,192.02
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-SS-1Y-USPP	$ 999,529.00	$ 869,590.23
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-SS-1Y-USPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-SS-1Y-USPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-SS-1Y-USPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-SS-1Y-USPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-SS-1Y-USPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-SS-1Y-USPP	$ 2,498,822.00	$ 2,173,975.14

FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-SS-1Y-USPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-SS-1Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-SS-1Y-USPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-SS-1Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-SS-1Y-USPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-SS-1Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-SS-2Y-USPP	$ 488,534.00	$ 425,024.58
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-SS-2Y-USPP	$ 580,142.00	$ 504,723.54
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-SS-2Y-USPP	$ 660,688.00	$ 574,798.56
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-SS-2Y-USPP	$ 999,528.00	$ 869,589.36
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-SS-2Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-SS-2Y-USPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-SS-2Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-SS-2Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-SS-2Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-SS-2Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-SS-2Y-USPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-SS-2Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-SS-2Y-USPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-SS-2Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-SS-2Y-USPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-SS-2Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-SS-2Y-USPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-SS-2Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-SS-3Y-USPP	$ 732,801.00	$ 637,536.87
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-SS-3Y-USPP	$ 870,213.00	$ 757,085.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-SS-3Y-USPP	$ 991,032.00	$ 862,197.84
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-SS-3Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-SS-3Y-USPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-SS-3Y-USPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-SS-3Y-USPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-SS-3Y-USPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-SS-3Y-USPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-SS-3Y-USPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-SS-3Y-USPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-SS-3Y-USPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-SS-3Y-USPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-SS-3Y-USPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-SS-3Y-USPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-SS-3Y-USPP	##############	$ 9,130,693.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-SS-3Y-USPP	##############	$ 9,782,885.52
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-SS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-SS-4Y-USPP	$ 977,068.00	$ 850,049.16
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-SS-4Y-USPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-SS-4Y-USPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-SS-4Y-USPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-SS-4Y-USPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-SS-4Y-USPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-SS-4Y-USPP	$ 4,997,644.00	$ 4,347,950.28

FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-SS-4Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-SS-4Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-SS-4Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-SS-4Y-USPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-SS-4Y-USPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-SS-4Y-USPP	##########	$ 9,565,489.92
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-SS-5Y-USPP	$ 1,221,335.00	$ 1,062,561.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-SS-5Y-USPP	$ 1,450,355.00	$ 1,261,808.85
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-SS-5Y-USPP	$ 1,651,720.00	$ 1,436,996.40
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-SS-5Y-USPP	$ 2,498,820.00	$ 2,173,973.40
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-SS-5Y-USPP	$ 3,748,230.00	$ 3,260,960.10
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-SS-5Y-USPP	$ 4,997,645.00	$ 4,347,951.15
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-SS-5Y-USPP	$ 6,247,055.00	$ 5,434,937.85
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-SS-5Y-USPP	$ 7,496,465.00	$ 6,521,924.55
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-SS-5Y-USPP	$ 8,745,875.00	$ 7,608,911.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-SS-5Y-USPP	$ 9,995,285.00	$ 8,695,897.95
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-SS-5Y-USPP	##########	$ 9,782,884.65
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-SS-5Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-1Y-USPP	$ 244,267.00	$ 212,512.29
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-1Y-USPP	$ 290,071.00	$ 252,361.77
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-1Y-USPP	$ 330,344.00	$ 287,399.28
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-1Y-USPP	$ 499,764.00	$ 434,794.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-1Y-USPP	$ 749,646.00	$ 652,192.02
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-1Y-USPP	$ 999,529.00	$ 869,590.23
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-1Y-USPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-1Y-USPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-1Y-USPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-1Y-USPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-1Y-USPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-1Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-1Y-USPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-1Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-1Y-USPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-1Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-1Y-USPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-1Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-2Y-USPP	$ 488,534.00	$ 425,024.58
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-2Y-USPP	$ 580,142.00	$ 504,723.54

FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-2Y-USPP	$ 660,688.00	$ 574,798.56
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-2Y-USPP	$ 999,528.00	$ 869,589.36
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-2Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-2Y-USPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-2Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-2Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-2Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-2Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-2Y-USPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-2Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-2Y-USPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-2Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-2Y-USPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-2Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-2Y-USPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-2Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-3Y-USPP	$ 732,801.00	$ 637,536.87
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-3Y-USPP	$ 870,213.00	$ 757,085.31
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-3Y-USPP	$ 991,032.00	$ 862,197.84
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-3Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-3Y-USPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-3Y-USPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-3Y-USPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-3Y-USPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-3Y-USPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-3Y-USPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-3Y-USPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-3Y-USPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-3Y-USPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-3Y-USPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-3Y-USPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-3Y-USPP	############	$ 9,130,693.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-3Y-USPP	############	$ 9,782,885.52
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-3Y-USPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-4Y-USPP	$ 977,068.00	$ 850,049.16
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-4Y-USPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-4Y-USPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-4Y-USPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-4Y-USPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-4Y-USPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-4Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-4Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-4Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-4Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-4Y-USPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-4Y-USPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-4Y-USPP	############	$ 9,565,489.92
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-4Y-USPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-4Y-USPP	############	############

FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-4Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-4Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-LS-1Y-US	$ 492,411.00	$ 428,397.57
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-LS-1Y-US	$ 600,978.00	$ 522,850.86
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-LS-1Y-US	$ 704,277.00	$ 612,720.99
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-LS-1Y-US	$ 1,125,406.00	$ 979,103.22
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-LS-1Y-US	$ 1,688,109.00	$ 1,468,654.83
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-LS-1Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-LS-1Y-US	$ 2,813,515.00	$ 2,447,758.05
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-LS-1Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-LS-1Y-US	$ 3,938,921.00	$ 3,426,861.27
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-LS-1Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-LS-2Y-US	$ 984,822.00	$ 856,795.14
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-LS-2Y-US	$ 1,201,956.00	$ 1,045,701.72
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-LS-2Y-US	$ 1,408,554.00	$ 1,225,441.98
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-LS-2Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-LS-2Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-LS-2Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-LS-2Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-LS-2Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-LS-2Y-US	$ 7,877,842.00	$ 6,853,722.54
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-LS-2Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-LS-3Y-US	$ 1,477,233.00	$ 1,285,192.71
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-LS-3Y-US	$ 1,802,934.00	$ 1,568,552.58
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-LS-3Y-US	$ 2,112,831.00	$ 1,838,162.97
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-LS-3Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-LS-3Y-US	$ 5,064,327.00	$ 4,405,964.49
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-LS-3Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-LS-3Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-LS-3Y-US	##########	$ 8,811,928.98
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-LS-3Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-LS-3Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-LS-4Y-US	$ 1,969,644.00	$ 1,713,590.28
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-LS-4Y-US	$ 2,403,912.00	$ 2,091,403.44
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-LS-4Y-US	$ 2,817,108.00	$ 2,450,883.96
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-LS-4Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-LS-4Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-LS-4Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-LS-4Y-US	##########	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-LS-5Y-US	$ 2,462,055.00	$ 2,141,987.85
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-LS-5Y-US	$ 3,004,890.00	$ 2,614,254.30
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-LS-5Y-US	$ 3,521,385.00	$ 3,063,604.95
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-LS-5Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-LS-5Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-LS-5Y-US	##########	$ 9,791,032.20

FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-LS-5Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-LS-5Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-LS-5Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-LS-5Y-US	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-LS-1Y-US	$ 492,411.00	$ 428,397.57
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-LS-1Y-US	$ 600,978.00	$ 522,850.86
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-LS-1Y-US	$ 704,277.00	$ 612,720.99
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-LS-1Y-US	$ 1,125,406.00	$ 979,103.22
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-LS-1Y-US	$ 1,688,109.00	$ 1,468,654.83
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-LS-1Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-LS-1Y-US	$ 2,813,515.00	$ 2,447,758.05
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-LS-1Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-LS-1Y-US	$ 3,938,921.00	$ 3,426,861.27
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-LS-1Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-LS-2Y-US	$ 984,822.00	$ 856,795.14
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-LS-2Y-US	$ 1,201,956.00	$ 1,045,701.72
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-LS-2Y-US	$ 1,408,554.00	$ 1,225,441.98
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-LS-2Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-LS-2Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-LS-2Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-LS-2Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-LS-2Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-LS-2Y-US	$ 7,877,842.00	$ 6,853,722.54
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-LS-2Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-LS-3Y-US	$ 1,477,233.00	$ 1,285,192.71
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-LS-3Y-US	$ 1,802,934.00	$ 1,568,552.58
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-LS-3Y-US	$ 2,112,831.00	$ 1,838,162.97
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-LS-3Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-LS-3Y-US	$ 5,064,327.00	$ 4,405,964.49
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-LS-3Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-LS-3Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-LS-3Y-US	##########	$ 8,811,928.98
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-LS-3Y-US	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-LS-3Y-US	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-LS-4Y-US	$ 1,969,644.00	$ 1,713,590.28
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-LS-4Y-US	$ 2,403,912.00	$ 2,091,403.44
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-LS-4Y-US	$ 2,817,108.00	$ 2,450,883.96
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-LS-4Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-LS-4Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-LS-4Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-LS-4Y-US	##########	$ 9,791,032.20
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-LS-4Y-US	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-LS-4Y-US	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-LS-1Y-USPP	$ 517,032.00	$ 449,817.84
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-LS-1Y-USPP	$ 631,027.00	$ 548,993.49
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-LS-1Y-USPP	$ 739,491.00	$ 643,357.17
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-LS-1Y-USPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-LS-1Y-USPP	$ 1,772,514.00	$ 1,542,087.18

FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-LS-1Y-USPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-LS-1Y-USPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-LS-1Y-USPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-LS-1Y-USPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-LS-1Y-USPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-LS-2Y-USPP	$ 1,034,064.00	$ 899,635.68
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-LS-2Y-USPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-LS-2Y-USPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-LS-2Y-USPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-LS-2Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-LS-2Y-USPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-LS-2Y-USPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-LS-2Y-USPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-LS-2Y-USPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-LS-2Y-USPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-LS-3Y-USPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-LS-3Y-USPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-LS-3Y-USPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-LS-3Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-LS-3Y-USPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-LS-3Y-USPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-LS-3Y-USPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-LS-3Y-USPP	##############	$ 9,252,525.69
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-LS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-LS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-LS-4Y-USPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-LS-4Y-USPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-LS-4Y-USPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-LS-4Y-USPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-LS-4Y-USPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-LS-4Y-USPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-LS-5Y-USPP	$ 2,585,160.00	$ 2,249,089.20
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-LS-5Y-USPP	$ 3,155,135.00	$ 2,744,967.45
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-LS-5Y-USPP	$ 3,697,455.00	$ 3,216,785.85
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-LS-5Y-USPP	$ 5,908,380.00	$ 5,140,290.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-LS-5Y-USPP	$ 8,862,570.00	$ 7,710,435.90
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-LS-5Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-1Y-USPP	$ 517,032.00	$ 449,817.84
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-1Y-USPP	$ 631,027.00	$ 548,993.49
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-1Y-USPP	$ 739,491.00	$ 643,357.17
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-1Y-USPP	$ 1,181,676.00	$ 1,028,058.12

FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-1Y-USPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-1Y-USPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-1Y-USPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-1Y-USPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-1Y-USPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-1Y-USPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-2Y-USPP	$ 1,034,064.00	$ 899,635.68
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-2Y-USPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-2Y-USPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-2Y-USPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-2Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-2Y-USPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-2Y-USPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-2Y-USPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-2Y-USPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-2Y-USPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-3Y-USPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-3Y-USPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-3Y-USPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-3Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-3Y-USPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-3Y-USPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-3Y-USPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-3Y-USPP	##############	$ 9,252,525.69
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-3Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-3Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-4Y-USPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-4Y-USPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-4Y-USPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-4Y-USPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-4Y-USPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-4Y-USPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - GovUS	TAP-1KEPS-DT2SS-1Y-US-A	$ 122,185.00	$ 106,300.95
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-DT2SS-1Y-US-A	$ 157,270.00	$ 136,824.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - GovUS	TAP-5KEPS-DT2SS-1Y-US-A	$ 193,405.00	$ 168,262.35
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - GovUS	TAP-10KEPS-DT2SS-1Y-US-A	$ 327,834.00	$ 285,215.58
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - GovUS	TAP-15KEPS-DT2SS-1Y-US-A	$ 491,751.00	$ 427,823.37
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - GovUS	TAP-20KEPS-DT2SS-1Y-US-A	$ 686,854.00	$ 597,562.98
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - GovUS	TAP-25KEPS-DT2SS-1Y-US-A	$ 875,135.00	$ 761,367.45
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - GovUS	TAP-30KEPS-DT2SS-1Y-US-A	$ 1,050,162.00	$ 913,640.94
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - GovUS	TAP-35KEPS-DT2SS-1Y-US-A	$ 1,225,189.00	$ 1,065,914.43
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - GovUS	TAP-40KEPS-DT2SS-1Y-US-A	$ 1,400,216.00	$ 1,218,187.92
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - GovUS	TAP-45KEPS-DT2SS-1Y-US-A	$ 1,575,243.00	$ 1,370,461.41
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - GovUS	TAP-50KEPS-DT2SS-1Y-US-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - GovUS	TAP-55KEPS-DT2SS-1Y-US-A	$ 1,925,297.00	$ 1,675,008.39

FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - GovUS	TAP-60KEPS-DT2SS-1Y-US-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - GovUS	TAP-65KEPS-DT2SS-1Y-US-A	$ 2,275,351.00	$ 1,979,555.37
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - GovUS	TAP-70KEPS-DT2SS-1Y-US-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - GovUS	TAP-75KEPS-DT2SS-1Y-US-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - GovUS	TAP-80KEPS-DT2SS-1Y-US-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - GovUS	TAP-1KEPS-DT2SS-2Y-US-A	$ 244,370.00	$ 212,601.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-DT2SS-2Y-US-A	$ 314,540.00	$ 273,649.80
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - GovUS	TAP-5KEPS-DT2SS-2Y-US-A	$ 386,810.00	$ 336,524.70
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - GovUS	TAP-10KEPS-DT2SS-2Y-US-A	$ 655,668.00	$ 570,431.16
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - GovUS	TAP-15KEPS-DT2SS-2Y-US-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - GovUS	TAP-20KEPS-DT2SS-2Y-US-A	$ 1,373,708.00	$ 1,195,125.96
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - GovUS	TAP-25KEPS-DT2SS-2Y-US-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - GovUS	TAP-30KEPS-DT2SS-2Y-US-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - GovUS	TAP-35KEPS-DT2SS-2Y-US-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - GovUS	TAP-40KEPS-DT2SS-2Y-US-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - GovUS	TAP-45KEPS-DT2SS-2Y-US-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - GovUS	TAP-50KEPS-DT2SS-2Y-US-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - GovUS	TAP-55KEPS-DT2SS-2Y-US-A	$ 3,850,594.00	$ 3,350,016.78
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - GovUS	TAP-60KEPS-DT2SS-2Y-US-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - GovUS	TAP-65KEPS-DT2SS-2Y-US-A	$ 4,550,702.00	$ 3,959,110.74
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - GovUS	TAP-70KEPS-DT2SS-2Y-US-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - GovUS	TAP-75KEPS-DT2SS-2Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - GovUS	TAP-80KEPS-DT2SS-2Y-US-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - GovUS	TAP-1KEPS-DT2SS-3Y-US-A	$ 366,555.00	$ 318,902.85
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-DT2SS-3Y-US-A	$ 471,810.00	$ 410,474.70
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - GovUS	TAP-5KEPS-DT2SS-3Y-US-A	$ 580,215.00	$ 504,787.05
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - GovUS	TAP-10KEPS-DT2SS-3Y-US-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - GovUS	TAP-15KEPS-DT2SS-3Y-US-A	$ 1,475,253.00	$ 1,283,470.11
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - GovUS	TAP-20KEPS-DT2SS-3Y-US-A	$ 2,060,562.00	$ 1,792,688.94
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - GovUS	TAP-25KEPS-DT2SS-3Y-US-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - GovUS	TAP-30KEPS-DT2SS-3Y-US-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - GovUS	TAP-35KEPS-DT2SS-3Y-US-A	$ 3,675,567.00	$ 3,197,743.29
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - GovUS	TAP-40KEPS-DT2SS-3Y-US-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - GovUS	TAP-45KEPS-DT2SS-3Y-US-A	$ 4,725,729.00	$ 4,111,384.23
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - GovUS	TAP-50KEPS-DT2SS-3Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - GovUS	TAP-55KEPS-DT2SS-3Y-US-A	$ 5,775,891.00	$ 5,025,025.17
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - GovUS	TAP-60KEPS-DT2SS-3Y-US-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - GovUS	TAP-65KEPS-DT2SS-3Y-US-A	$ 6,826,053.00	$ 5,938,666.11
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - GovUS	TAP-70KEPS-DT2SS-3Y-US-A	$ 7,351,134.00	$ 6,395,486.58
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - GovUS	TAP-75KEPS-DT2SS-3Y-US-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - GovUS	TAP-80KEPS-DT2SS-3Y-US-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - GovUS	TAP-1KEPS-DT2SS-4Y-US-A	$ 488,740.00	$ 425,203.80
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-DT2SS-4Y-US-A	$ 629,080.00	$ 547,299.60
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - GovUS	TAP-5KEPS-DT2SS-4Y-US-A	$ 773,620.00	$ 673,049.40
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - GovUS	TAP-10KEPS-DT2SS-4Y-US-A	$ 1,311,336.00	$ 1,140,862.32
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - GovUS	TAP-15KEPS-DT2SS-4Y-US-A	$ 1,967,004.00	$ 1,711,293.48
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - GovUS	TAP-20KEPS-DT2SS-4Y-US-A	$ 2,747,416.00	$ 2,390,251.92
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - GovUS	TAP-25KEPS-DT2SS-4Y-US-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - GovUS	TAP-30KEPS-DT2SS-4Y-US-A	$ 4,200,648.00	$ 3,654,563.76

FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - GovUS	TAP-35KEPS-DT2SS-4Y-US-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - GovUS	TAP-40KEPS-DT2SS-4Y-US-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - GovUS	TAP-45KEPS-DT2SS-4Y-US-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - GovUS	TAP-50KEPS-DT2SS-4Y-US-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - GovUS	TAP-55KEPS-DT2SS-4Y-US-A	$ 7,701,188.00	$ 6,700,033.56
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - GovUS	TAP-60KEPS-DT2SS-4Y-US-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - GovUS	TAP-65KEPS-DT2SS-4Y-US-A	$ 9,101,404.00	$ 7,918,221.48
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - GovUS	TAP-70KEPS-DT2SS-4Y-US-A	$ 9,801,512.00	$ 8,527,315.44
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - GovUS	TAP-75KEPS-DT2SS-4Y-US-A	############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - GovUS	TAP-80KEPS-DT2SS-4Y-US-A	############	$ 9,745,503.36
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - GovUS	TAP-1KEPS-DT2SS-5Y-US-A	$ 610,925.00	$ 531,504.75
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-DT2SS-5Y-US-A	$ 786,350.00	$ 684,124.50
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - GovUS	TAP-5KEPS-DT2SS-5Y-US-A	$ 967,025.00	$ 841,311.75
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - GovUS	TAP-10KEPS-DT2SS-5Y-US-A	$ 1,639,170.00	$ 1,426,077.90
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - GovUS	TAP-15KEPS-DT2SS-5Y-US-A	$ 2,458,755.00	$ 2,139,116.85
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - GovUS	TAP-20KEPS-DT2SS-5Y-US-A	$ 3,434,270.00	$ 2,987,814.90
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - GovUS	TAP-25KEPS-DT2SS-5Y-US-A	$ 4,375,675.00	$ 3,806,837.25
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - GovUS	TAP-30KEPS-DT2SS-5Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - GovUS	TAP-35KEPS-DT2SS-5Y-US-A	$ 6,125,945.00	$ 5,329,572.15
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - GovUS	TAP-40KEPS-DT2SS-5Y-US-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - GovUS	TAP-45KEPS-DT2SS-5Y-US-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - GovUS	TAP-50KEPS-DT2SS-5Y-US-A	$ 8,751,350.00	$ 7,613,674.50
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - GovUS	TAP-55KEPS-DT2SS-5Y-US-A	$ 9,626,485.00	$ 8,375,041.95
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - GovUS	TAP-60KEPS-DT2SS-5Y-US-A	############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - GovUS	TAP-65KEPS-DT2SS-5Y-US-A	############	$ 9,897,776.85
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - GovUS	TAP-70KEPS-DT2SS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - GovUS	TAP-75KEPS-DT2SS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - GovUS	TAP-80KEPS-DT2SS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-1Y-USPP-A	$ 128,294.00	$ 111,615.78
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-1Y-USPP	$ 165,134.00	$ 143,666.58
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-1Y-USPP-A	$ 203,076.00	$ 176,676.12
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-1Y-USPP-	$ 344,225.00	$ 299,475.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-1Y-USPP-	$ 516,338.00	$ 449,214.06
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-1Y-USPP-	$ 721,197.00	$ 627,441.39
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-1Y-USPP-	$ 918,892.00	$ 799,436.04
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-1Y-USPP-	$ 1,102,670.00	$ 959,322.90
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-1Y-USPP-	$ 1,286,448.00	$ 1,119,209.76
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-1Y-USPP-	$ 1,470,227.00	$ 1,279,097.49
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-1Y-USPP-	$ 1,654,005.00	$ 1,438,984.35
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-1Y-USPP-	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-1Y-USPP-	$ 2,021,562.00	$ 1,758,758.94
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-1Y-USPP-	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-1Y-USPP-	$ 2,389,119.00	$ 2,078,533.53
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-1Y-USPP-	$ 2,572,897.00	$ 2,238,420.39
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-1Y-USPP-	$ 2,756,675.00	$ 2,398,307.25
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-1Y-USPP-	$ 2,940,453.00	$ 2,558,194.11
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-2Y-USPP-A	$ 256,588.00	$ 223,231.56
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-2Y-USPP	$ 330,268.00	$ 287,333.16
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-2Y-USPP-A	$ 406,152.00	$ 353,352.24

FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-2Y-USPP-	$ 688,450.00	$ 598,951.50
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-2Y-USPP-	$ 1,032,676.00	$ 898,428.12
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-2Y-USPP-	$ 1,442,394.00	$ 1,254,882.78
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-2Y-USPP-	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-2Y-USPP-	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-2Y-USPP-	$ 2,572,896.00	$ 2,238,419.52
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-2Y-USPP-	$ 2,940,454.00	$ 2,558,194.98
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-2Y-USPP-	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-2Y-USPP-	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-2Y-USPP-	$ 4,043,124.00	$ 3,517,517.88
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-2Y-USPP-	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-2Y-USPP-	$ 4,778,238.00	$ 4,157,067.06
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-2Y-USPP-	$ 5,145,794.00	$ 4,476,840.78
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-2Y-USPP-	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-2Y-USPP-	$ 5,880,906.00	$ 5,116,388.22
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-3Y-USPP-A	$ 384,882.00	$ 334,847.34
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-3Y-USPP	$ 495,402.00	$ 430,999.74
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-3Y-USPP-A	$ 609,228.00	$ 530,028.36
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-3Y-USPP-	$ 1,032,675.00	$ 898,427.25
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-3Y-USPP-	$ 1,549,014.00	$ 1,347,642.18
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-3Y-USPP-	$ 2,163,591.00	$ 1,882,324.17
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-3Y-USPP-	$ 2,756,676.00	$ 2,398,308.12
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-3Y-USPP-	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-3Y-USPP-	$ 3,859,344.00	$ 3,357,629.28
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-3Y-USPP-	$ 4,410,681.00	$ 3,837,292.47
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-3Y-USPP-	$ 4,962,015.00	$ 4,316,953.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-3Y-USPP-	$ 5,513,352.00	$ 4,796,616.24
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-3Y-USPP-	$ 6,064,686.00	$ 5,276,276.82
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-3Y-USPP-	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-3Y-USPP-	$ 7,167,357.00	$ 6,235,600.59
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-3Y-USPP-	$ 7,718,691.00	$ 6,715,261.17
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-3Y-USPP-	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-3Y-USPP-	$ 8,821,359.00	$ 7,674,582.33
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-4Y-USPP-A	$ 513,176.00	$ 446,463.12
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-4Y-USPP	$ 660,536.00	$ 574,666.32
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-4Y-USPP-A	$ 812,304.00	$ 706,704.48
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-4Y-USPP-	$ 1,376,900.00	$ 1,197,903.00
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-4Y-USPP-	$ 2,065,352.00	$ 1,796,856.24
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-4Y-USPP-	$ 2,884,788.00	$ 2,509,765.56
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-4Y-USPP-	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-4Y-USPP-	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-4Y-USPP-	$ 5,145,792.00	$ 4,476,839.04
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-4Y-USPP-	$ 5,880,908.00	$ 5,116,389.96
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-4Y-USPP-	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-4Y-USPP-	$ 7,351,136.00	$ 6,395,488.32
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-4Y-USPP-	$ 8,086,248.00	$ 7,035,035.76
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-4Y-USPP-	$ 8,821,360.00	$ 7,674,583.20
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-4Y-USPP-	$ 9,556,476.00	$ 8,314,134.12
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-4Y-USPP-	##############	$ 8,953,681.56

FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-4Y-USPP-	##########	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-5Y-USPP-A	$ 641,470.00	$ 558,078.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-5Y-USPP	$ 825,670.00	$ 718,332.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-5Y-USPP-A	$ 1,015,380.00	$ 883,380.60
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-5Y-USPP-	$ 1,721,125.00	$ 1,497,378.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-5Y-USPP-	$ 2,581,690.00	$ 2,246,070.30
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-5Y-USPP-	$ 3,605,985.00	$ 3,137,206.95
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-5Y-USPP-	$ 4,594,460.00	$ 3,997,180.20
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-5Y-USPP-	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-5Y-USPP-	$ 6,432,240.00	$ 5,596,048.80
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-5Y-USPP-	$ 7,351,135.00	$ 6,395,487.45
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-5Y-USPP-	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-5Y-USPP-	$ 9,188,920.00	$ 7,994,360.40
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-5Y-USPP-	##########	$ 8,793,794.70
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-5Y-USPP-	##########	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-DT2LS-1Y-US-A	$ 381,961.00	$ 332,306.07
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-DT2LS-1Y-US-A	$ 481,990.00	$ 419,331.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-DT2LS-1Y-US-A	$ 583,069.00	$ 507,270.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-DT2LS-1Y-US-A	$ 977,274.00	$ 850,228.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-DT2LS-1Y-US-A	$ 1,465,911.00	$ 1,275,342.57
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-DT2LS-1Y-US-A	$ 1,985,734.00	$ 1,727,588.58
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-DT2LS-1Y-US-A	$ 2,498,735.00	$ 2,173,899.45
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-DT2LS-1Y-US-A	$ 2,998,482.00	$ 2,608,679.34
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-DT2LS-1Y-US-A	$ 3,498,229.00	$ 3,043,459.23
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-DT2LS-1Y-US-A	$ 3,997,976.00	$ 3,478,239.12
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-DT2LS-2Y-US-A	$ 763,922.00	$ 664,612.14
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-DT2LS-2Y-US-A	$ 963,980.00	$ 838,662.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-DT2LS-2Y-US-A	$ 1,166,138.00	$ 1,014,540.06
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-DT2LS-2Y-US-A	$ 1,954,548.00	$ 1,700,456.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-DT2LS-2Y-US-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-DT2LS-2Y-US-A	$ 3,971,468.00	$ 3,455,177.16
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-DT2LS-2Y-US-A	$ 4,997,470.00	$ 4,347,798.90
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-DT2LS-2Y-US-A	$ 5,996,964.00	$ 5,217,358.68
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-DT2LS-2Y-US-A	$ 6,996,458.00	$ 6,086,918.46
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-DT2LS-2Y-US-A	$ 7,995,952.00	$ 6,956,478.24
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-DT2LS-3Y-US-A	$ 1,145,883.00	$ 996,918.21
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-DT2LS-3Y-US-A	$ 1,445,970.00	$ 1,257,993.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-DT2LS-3Y-US-A	$ 1,749,207.00	$ 1,521,810.09
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-DT2LS-3Y-US-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-DT2LS-3Y-US-A	$ 4,397,733.00	$ 3,826,027.71
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-DT2LS-3Y-US-A	$ 5,957,202.00	$ 5,182,765.74
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-DT2LS-3Y-US-A	$ 7,496,205.00	$ 6,521,698.35
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-DT2LS-3Y-US-A	$ 8,995,446.00	$ 7,826,038.02
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-DT2LS-3Y-US-A	##########	$ 9,130,377.69

FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-DT2LS-3Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-DT2LS-4Y-US-A	$ 1,527,844.00	$ 1,329,224.28
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-DT2LS-4Y-US-A	$ 1,927,960.00	$ 1,677,325.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-DT2LS-4Y-US-A	$ 2,332,276.00	$ 2,029,080.12
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-DT2LS-4Y-US-A	$ 3,909,096.00	$ 3,400,913.52
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-DT2LS-4Y-US-A	$ 5,863,644.00	$ 5,101,370.28
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-DT2LS-4Y-US-A	$ 7,942,936.00	$ 6,910,354.32
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-DT2LS-4Y-US-A	$ 9,994,940.00	$ 8,695,597.80
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-DT2LS-5Y-US-A	$ 1,909,805.00	$ 1,661,530.35
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-DT2LS-5Y-US-A	$ 2,409,950.00	$ 2,096,656.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-DT2LS-5Y-US-A	$ 2,915,345.00	$ 2,536,350.15
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-DT2LS-5Y-US-A	$ 4,886,370.00	$ 4,251,141.90
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-DT2LS-5Y-US-A	$ 7,329,555.00	$ 6,376,712.85
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-DT2LS-5Y-US-A	$ 9,928,670.00	$ 8,637,942.90
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-1Y-USPP-A	$ 401,059.00	$ 348,921.33
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-1Y-USPP	$ 506,090.00	$ 440,298.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-1Y-USPP-A	$ 612,223.00	$ 532,634.01
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-1Y-USPP-	$ 1,026,137.00	$ 892,739.19
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-1Y-USPP-	$ 1,539,206.00	$ 1,339,109.22
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-1Y-USPP-	$ 2,085,021.00	$ 1,813,968.27
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-1Y-USPP-	$ 2,623,672.00	$ 2,282,594.64
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-1Y-USPP-	$ 3,148,406.00	$ 2,739,113.22
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-1Y-USPP-	$ 3,673,140.00	$ 3,195,631.80
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-1Y-USPP-	$ 4,197,875.00	$ 3,652,151.25
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-2Y-USPP-A	$ 802,118.00	$ 697,842.66
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-2Y-USPP	$ 1,012,180.00	$ 880,596.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-2Y-USPP-A	$ 1,224,446.00	$ 1,065,268.02
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-2Y-USPP-	$ 2,052,274.00	$ 1,785,478.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-2Y-USPP-	$ 3,078,412.00	$ 2,678,218.44
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-2Y-USPP-	$ 4,170,042.00	$ 3,627,936.54
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-2Y-USPP-	$ 5,247,344.00	$ 4,565,189.28
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-2Y-USPP-	$ 6,296,812.00	$ 5,478,226.44
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-2Y-USPP-	$ 7,346,280.00	$ 6,391,263.60
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-2Y-USPP-	$ 8,395,750.00	$ 7,304,302.50
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-3Y-USPP-A	$ 1,203,177.00	$ 1,046,763.99
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-3Y-USPP	$ 1,518,270.00	$ 1,320,894.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-3Y-USPP-A	$ 1,836,669.00	$ 1,597,902.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-3Y-USPP-	$ 3,078,411.00	$ 2,678,217.57
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-3Y-USPP-	$ 4,617,618.00	$ 4,017,327.66
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-3Y-USPP-	$ 6,255,063.00	$ 5,441,904.81
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-3Y-USPP-	$ 7,871,016.00	$ 6,847,783.92
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-3Y-USPP-	$ 9,445,218.00	$ 8,217,339.66

FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-3Y-USPP-	##########	$ 9,586,895.40
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-3Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-4Y-USPP-A	$ 1,604,236.00	$ 1,395,685.32
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-4Y-USPP	$ 2,024,360.00	$ 1,761,193.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-4Y-USPP-A	$ 2,448,892.00	$ 2,130,536.04
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-4Y-USPP-	$ 4,104,548.00	$ 3,570,956.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-4Y-USPP-	$ 6,156,824.00	$ 5,356,436.88
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-4Y-USPP-	$ 8,340,084.00	$ 7,255,873.08
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-4Y-USPP-	##########	$ 9,130,378.56
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-5Y-USPP-A	$ 2,005,295.00	$ 1,744,606.65
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-5Y-USPP	$ 2,530,450.00	$ 2,201,491.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-5Y-USPP-A	$ 3,061,115.00	$ 2,663,170.05
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-5Y-USPP-	$ 5,130,685.00	$ 4,463,695.95
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-5Y-USPP-	$ 7,696,030.00	$ 6,695,546.10
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-5Y-USPP-	##########	$ 9,069,841.35
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-SS2LS-1Y-US-A	$ 259,776.00	$ 226,005.12
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-SS2LS-1Y-US-A	$ 324,720.00	$ 282,506.40
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-SS2LS-1Y-US-A	$ 389,664.00	$ 339,007.68
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-SS2LS-1Y-US-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-SS2LS-1Y-US-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-SS2LS-1Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-SS2LS-1Y-US-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-SS2LS-1Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-SS2LS-1Y-US-A	$ 2,273,040.00	$ 1,977,544.80
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-SS2LS-1Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-SS2LS-2Y-US-A	$ 519,552.00	$ 452,010.24
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-SS2LS-2Y-US-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-SS2LS-2Y-US-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-SS2LS-2Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-SS2LS-2Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-SS2LS-2Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-SS2LS-2Y-US-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-SS2LS-2Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-SS2LS-2Y-US-A	$ 4,546,080.00	$ 3,955,089.60
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-SS2LS-2Y-US-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-SS2LS-3Y-US-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-SS2LS-3Y-US-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-SS2LS-3Y-US-A	$ 1,168,992.00	$ 1,017,023.04
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-SS2LS-3Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-SS2LS-3Y-US-A	$ 2,922,480.00	$ 2,542,557.60
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-SS2LS-3Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-SS2LS-3Y-US-A	$ 4,870,800.00	$ 4,237,596.00

FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-SS2LS-3Y-US-A	$ 5,844,960.00	$ 5,085,115.20
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-SS2LS-3Y-US-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-SS2LS-3Y-US-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-SS2LS-4Y-US-A	$ 1,039,104.00	$ 904,020.48
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-SS2LS-4Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-SS2LS-4Y-US-A	$ 1,558,656.00	$ 1,356,030.72
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-SS2LS-4Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-SS2LS-4Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-SS2LS-4Y-US-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-SS2LS-4Y-US-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-SS2LS-4Y-US-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-SS2LS-4Y-US-A	$ 9,092,160.00	$ 7,910,179.20
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-SS2LS-4Y-US-A	##############	$ 9,040,204.80
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-SS2LS-5Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-SS2LS-5Y-US-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-SS2LS-5Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-SS2LS-5Y-US-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-SS2LS-5Y-US-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-SS2LS-5Y-US-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-SS2LS-5Y-US-A	$ 8,118,000.00	$ 7,062,660.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-SS2LS-5Y-US-A	$ 9,741,600.00	$ 8,475,192.00
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-SS2LS-5Y-US-A	##############	$ 9,887,724.00
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-SS2LS-5Y-US-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-1Y-USPP-A	$ 272,765.00	$ 237,305.55
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-1Y-USPP-	$ 340,956.00	$ 296,631.72
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-1Y-USPP-A	$ 409,147.00	$ 355,957.89
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-1Y-USPP-	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-1Y-USPP-	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-1Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-1Y-USPP-	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-1Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-1Y-USPP-	$ 2,386,692.00	$ 2,076,422.04
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-1Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-2Y-USPP-A	$ 545,530.00	$ 474,611.10
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-2Y-USPP-	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-2Y-USPP-A	$ 818,294.00	$ 711,915.78
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-2Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-2Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-2Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-2Y-USPP-	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-2Y-USPP-	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-2Y-USPP-	$ 4,773,384.00	$ 4,152,844.08
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-2Y-USPP-	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-3Y-USPP-A	$ 818,295.00	$ 711,916.65
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-3Y-USPP-	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-3Y-USPP-A	$ 1,227,441.00	$ 1,067,873.67
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-3Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-3Y-USPP-	$ 3,068,604.00	$ 2,669,685.48
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-3Y-USPP-	$ 4,091,472.00	$ 3,559,580.64

FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-3Y-USPP-	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-3Y-USPP-	$ 6,137,208.00	$ 5,339,370.96
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-3Y-USPP-	$ 7,160,076.00	$ 6,229,266.12
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-3Y-USPP-	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-4Y-USPP-A	$ 1,091,060.00	$ 949,222.20
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-4Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-4Y-USPP-A	$ 1,636,588.00	$ 1,423,831.56
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-4Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-4Y-USPP-	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-4Y-USPP-	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-4Y-USPP-	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-4Y-USPP-	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-4Y-USPP-	$ 9,546,768.00	$ 8,305,688.16
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-4Y-USPP-	##############	$ 9,492,215.04
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-5Y-USPP-A	$ 1,363,825.00	$ 1,186,527.75
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-5Y-USPP-	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-5Y-USPP-A	$ 2,045,735.00	$ 1,779,789.45
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-5Y-USPP-	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-5Y-USPP-	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-5Y-USPP-	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-5Y-USPP-	$ 8,523,900.00	$ 7,415,793.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-5Y-USPP-	##############	$ 8,898,951.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-5Y-USPP-	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-5Y-USPP-	##############	##############
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-1Y-PT2PP	$ 5,523.00	$ 4,805.01
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-1Y-PT2P	$ 5,949.00	$ 5,175.63
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-1Y-PT2PP	$ 6,060.00	$ 5,272.20
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-1Y-PT2P	$ 7,407.00	$ 6,444.09
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-1Y-PT2P	$ 11,110.00	$ 9,665.70
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-1Y-PT2P	$ 13,254.00	$ 11,530.98
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-1Y-PT2P	$ 15,739.00	$ 13,692.93
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-1Y-PT2P	$ 18,887.00	$ 16,431.69
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-1Y-PT2P	$ 22,035.00	$ 19,170.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-1Y-PT2P	$ 25,182.00	$ 21,908.34
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-1Y-PT2P	$ 28,330.00	$ 24,647.10
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-1Y-PT2P	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-1Y-PT2P	$ 34,626.00	$ 30,124.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-1Y-PT2P	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-1Y-PT2P	$ 40,921.00	$ 35,601.27
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-1Y-PT2P	$ 44,069.00	$ 38,340.03
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-1Y-PT2P	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-1Y-PT2P	$ 50,365.00	$ 43,817.55
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-2Y-PT2PP	$ 11,046.00	$ 9,610.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-2Y-PT2P	$ 11,898.00	$ 10,351.26
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-2Y-PT2PP	$ 12,120.00	$ 10,544.40
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-2Y-PT2P	$ 14,814.00	$ 12,888.18
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-2Y-PT2P	$ 22,220.00	$ 19,331.40
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-2Y-PT2P	$ 26,508.00	$ 23,061.96
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-2Y-PT2P	$ 31,478.00	$ 27,385.86

FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-2Y-PT2P	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-2Y-PT2P	$ 44,070.00	$ 38,340.90
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-2Y-PT2P	$ 50,364.00	$ 43,816.68
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-2Y-PT2P	$ 56,660.00	$ 49,294.20
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-2Y-PT2P	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-2Y-PT2P	$ 69,252.00	$ 60,249.24
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-2Y-PT2P	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-2Y-PT2P	$ 81,842.00	$ 71,202.54
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-2Y-PT2P	$ 88,138.00	$ 76,680.06
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-2Y-PT2P	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-2Y-PT2P	$ 100,730.00	$ 87,635.10
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-3Y-PT2PP	$ 16,569.00	$ 14,415.03
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-3Y-PT2P	$ 17,847.00	$ 15,526.89
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-3Y-PT2PP	$ 18,180.00	$ 15,816.60
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-3Y-PT2P	$ 22,221.00	$ 19,332.27
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-3Y-PT2P	$ 33,330.00	$ 28,997.10
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-3Y-PT2P	$ 39,762.00	$ 34,592.94
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-3Y-PT2P	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-3Y-PT2P	$ 56,661.00	$ 49,295.07
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-3Y-PT2P	$ 66,105.00	$ 57,511.35
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-3Y-PT2P	$ 75,546.00	$ 65,725.02
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-3Y-PT2P	$ 84,990.00	$ 73,941.30
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-3Y-PT2P	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-3Y-PT2P	$ 103,878.00	$ 90,373.86
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-3Y-PT2P	$ 113,322.00	$ 98,590.14
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-3Y-PT2P	$ 122,763.00	$ 106,803.81
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-3Y-PT2P	$ 132,207.00	$ 115,020.09
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-3Y-PT2P	$ 141,651.00	$ 123,236.37
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-3Y-PT2P	$ 151,095.00	$ 131,452.65
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-4Y-PT2PP	$ 22,092.00	$ 19,220.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-4Y-PT2P	$ 23,796.00	$ 20,702.52
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-4Y-PT2PP	$ 24,240.00	$ 21,088.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-4Y-PT2P	$ 29,628.00	$ 25,776.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-4Y-PT2P	$ 44,440.00	$ 38,662.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-4Y-PT2P	$ 53,016.00	$ 46,123.92
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-4Y-PT2P	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-4Y-PT2P	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-4Y-PT2P	$ 88,140.00	$ 76,681.80
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-4Y-PT2P	$ 100,728.00	$ 87,633.36
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-4Y-PT2P	$ 113,320.00	$ 98,588.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-4Y-PT2P	$ 125,912.00	$ 109,543.44
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-4Y-PT2P	$ 138,504.00	$ 120,498.48
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-4Y-PT2P	$ 151,096.00	$ 131,453.52
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-4Y-PT2P	$ 163,684.00	$ 142,405.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-4Y-PT2P	$ 176,276.00	$ 153,360.12
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-4Y-PT2P	$ 188,868.00	$ 164,315.16
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-4Y-PT2P	$ 201,460.00	$ 175,270.20
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-5Y-PT2PP	$ 27,615.00	$ 24,025.05
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-5Y-PT2P	$ 29,745.00	$ 25,878.15

FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-5Y-PT2PP	$ 30,300.00	$ 26,361.00
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-5Y-PT2P	$ 37,035.00	$ 32,220.45
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-5Y-PT2P	$ 55,550.00	$ 48,328.50
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-5Y-PT2P	$ 66,270.00	$ 57,654.90
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-5Y-PT2P	$ 78,695.00	$ 68,464.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-5Y-PT2P	$ 94,435.00	$ 82,158.45
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-5Y-PT2P	$ 110,175.00	$ 95,852.25
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-5Y-PT2P	$ 125,910.00	$ 109,541.70
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-5Y-PT2P	$ 141,650.00	$ 123,235.50
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-5Y-PT2P	$ 157,390.00	$ 136,929.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-5Y-PT2P	$ 173,130.00	$ 150,623.10
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-5Y-PT2P	$ 188,870.00	$ 164,316.90
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-5Y-PT2P	$ 204,605.00	$ 178,006.35
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-5Y-PT2P	$ 220,345.00	$ 191,700.15
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-5Y-PT2P	$ 236,085.00	$ 205,393.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-5Y-PT2P	$ 251,825.00	$ 219,087.75
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-1Y-PT2PPP	$ 11,632.00	$ 10,119.84
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-1Y-PT2P	$ 13,813.00	$ 12,017.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-1Y-PT2PPP	$ 15,731.00	$ 13,685.97
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-1Y-PT2PP	$ 23,798.00	$ 20,704.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-1Y-PT2PP	$ 35,697.00	$ 31,056.39
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-1Y-PT2PP	$ 47,597.00	$ 41,409.39
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-1Y-PT2PP	$ 59,496.00	$ 51,761.52
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-1Y-PT2PP	$ 71,395.00	$ 62,113.65
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-1Y-PT2PP	$ 83,294.00	$ 72,465.78
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-1Y-PT2PP	$ 95,193.00	$ 82,817.91
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-1Y-PT2PP	$ 107,092.00	$ 93,170.04
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-1Y-PT2PP	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-1Y-PT2PP	$ 130,891.00	$ 113,875.17
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-1Y-PT2PP	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-1Y-PT2PP	$ 154,689.00	$ 134,579.43
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-1Y-PT2PP	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-1Y-PT2PP	$ 178,487.00	$ 155,283.69
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-1Y-PT2PP	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-2Y-PT2PPP	$ 23,264.00	$ 20,239.68
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-2Y-PT2P	$ 27,626.00	$ 24,034.62
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-2Y-PT2PPP	$ 31,462.00	$ 27,371.94
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-2Y-PT2PP	$ 47,596.00	$ 41,408.52
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-2Y-PT2PP	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-2Y-PT2PP	$ 95,194.00	$ 82,818.78
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-2Y-PT2PP	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-2Y-PT2PP	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-2Y-PT2PP	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-2Y-PT2PP	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-2Y-PT2PP	$ 214,184.00	$ 186,340.08
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-2Y-PT2PP	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-2Y-PT2PP	$ 261,782.00	$ 227,750.34
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-2Y-PT2PP	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-2Y-PT2PP	$ 309,378.00	$ 269,158.86

FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-2Y-PT2PP	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-2Y-PT2PP	$ 356,974.00	$ 310,567.38
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-2Y-PT2PP	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-3Y-PT2PPP	$ 34,896.00	$ 30,359.52
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-3Y-PT2P	$ 41,439.00	$ 36,051.93
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-3Y-PT2PPP	$ 47,193.00	$ 41,057.91
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-3Y-PT2PP	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-3Y-PT2PP	$ 107,091.00	$ 93,169.17
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-3Y-PT2PP	$ 142,791.00	$ 124,228.17
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-3Y-PT2PP	$ 178,488.00	$ 155,284.56
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-3Y-PT2PP	$ 214,185.00	$ 186,340.95
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-3Y-PT2PP	$ 249,882.00	$ 217,397.34
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-3Y-PT2PP	$ 285,579.00	$ 248,453.73
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-3Y-PT2PP	$ 321,276.00	$ 279,510.12
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-3Y-PT2PP	$ 356,976.00	$ 310,569.12
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-3Y-PT2PP	$ 392,673.00	$ 341,625.51
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-3Y-PT2PP	$ 428,370.00	$ 372,681.90
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-3Y-PT2PP	$ 464,067.00	$ 403,738.29
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-3Y-PT2PP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-3Y-PT2PP	$ 535,461.00	$ 465,851.07
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-3Y-PT2PP	$ 571,158.00	$ 496,907.46
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-4Y-PT2PPP	$ 46,528.00	$ 40,479.36
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-4Y-PT2P	$ 55,252.00	$ 48,069.24
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-4Y-PT2PPP	$ 62,924.00	$ 54,743.88
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-4Y-PT2PP	$ 95,192.00	$ 82,817.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-4Y-PT2PP	$ 142,788.00	$ 124,225.56
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-4Y-PT2PP	$ 190,388.00	$ 165,637.56
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-4Y-PT2PP	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-4Y-PT2PP	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-4Y-PT2PP	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-4Y-PT2PP	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-4Y-PT2PP	$ 428,368.00	$ 372,680.16
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-4Y-PT2PP	$ 475,968.00	$ 414,092.16
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-4Y-PT2PP	$ 523,564.00	$ 455,500.68
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-4Y-PT2PP	$ 571,160.00	$ 496,909.20
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-4Y-PT2PP	$ 618,756.00	$ 538,317.72
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-4Y-PT2PP	$ 666,352.00	$ 579,726.24
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-4Y-PT2PP	$ 713,948.00	$ 621,134.76
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-4Y-PT2PP	$ 761,544.00	$ 662,543.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-5Y-PT2PPP	$ 58,160.00	$ 50,599.20
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-5Y-PT2P	$ 69,065.00	$ 60,086.55
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-5Y-PT2PPP	$ 78,655.00	$ 68,429.85
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-5Y-PT2PP	$ 118,990.00	$ 103,521.30
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-5Y-PT2PP	$ 178,485.00	$ 155,281.95
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-5Y-PT2PP	$ 237,985.00	$ 207,046.95
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-5Y-PT2PP	$ 297,480.00	$ 258,807.60
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-5Y-PT2PP	$ 356,975.00	$ 310,568.25
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-5Y-PT2PP	$ 416,470.00	$ 362,328.90
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-5Y-PT2PP	$ 475,965.00	$ 414,089.55

FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-5Y-PT2PP	$ 535,460.00	$ 465,850.20
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-5Y-PT2PP	$ 594,960.00	$ 517,615.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-5Y-PT2PP	$ 654,455.00	$ 569,375.85
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-5Y-PT2PP	$ 713,950.00	$ 621,136.50
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-5Y-PT2PP	$ 773,445.00	$ 672,897.15
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-5Y-PT2PP	$ 832,940.00	$ 724,657.80
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-5Y-PT2PP	$ 892,435.00	$ 776,418.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-5Y-PT2PP	$ 951,930.00	$ 828,179.10
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-1Y-PT2PPP	$ 24,621.00	$ 21,420.27
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-1Y-PT2P	$ 30,049.00	$ 26,142.63
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-1Y-PT2PPP	$ 35,214.00	$ 30,636.18
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-1Y-PT2PP	$ 56,270.00	$ 48,954.90
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-1Y-PT2PP	$ 84,405.00	$ 73,432.35
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-1Y-PT2PP	$ 112,541.00	$ 97,910.67
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-1Y-PT2PP	$ 140,676.00	$ 122,388.12
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-1Y-PT2PP	$ 168,811.00	$ 146,865.57
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-1Y-PT2PP	$ 196,946.00	$ 171,343.02
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-1Y-PT2PP	$ 225,081.00	$ 195,820.47
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-2Y-PT2PPP	$ 49,242.00	$ 42,840.54
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-2Y-PT2P	$ 60,098.00	$ 52,285.26
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-2Y-PT2PPP	$ 70,428.00	$ 61,272.36
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-2Y-PT2PP	$ 112,540.00	$ 97,909.80
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-2Y-PT2PP	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-2Y-PT2PP	$ 225,082.00	$ 195,821.34
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-2Y-PT2PP	$ 281,352.00	$ 244,776.24
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-2Y-PT2PP	$ 337,622.00	$ 293,731.14
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-2Y-PT2PP	$ 393,892.00	$ 342,686.04
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-2Y-PT2PP	$ 450,162.00	$ 391,640.94
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-3Y-PT2PPP	$ 73,863.00	$ 64,260.81
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-3Y-PT2P	$ 90,147.00	$ 78,427.89
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-3Y-PT2PPP	$ 105,642.00	$ 91,908.54
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-3Y-PT2PP	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-3Y-PT2PP	$ 253,215.00	$ 220,297.05
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-3Y-PT2PP	$ 337,623.00	$ 293,732.01
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-3Y-PT2PP	$ 422,028.00	$ 367,164.36
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-3Y-PT2PP	$ 506,433.00	$ 440,596.71
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-3Y-PT2PP	$ 590,838.00	$ 514,029.06
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-3Y-PT2PP	$ 675,243.00	$ 587,461.41
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-4Y-PT2PPP	$ 98,484.00	$ 85,681.08
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-4Y-PT2P	$ 120,196.00	$ 104,570.52
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-4Y-PT2PPP	$ 140,856.00	$ 122,544.72
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-4Y-PT2PP	$ 225,080.00	$ 195,819.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-4Y-PT2PP	$ 337,620.00	$ 293,729.40
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-4Y-PT2PP	$ 450,164.00	$ 391,642.68
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-4Y-PT2PP	$ 562,704.00	$ 489,552.48
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-4Y-PT2PP	$ 675,244.00	$ 587,462.28
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-4Y-PT2PP	$ 787,784.00	$ 685,372.08
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-4Y-PT2PP	$ 900,324.00	$ 783,281.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-5Y-PT2PPP	$ 123,105.00	$ 107,101.35

FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-5Y-PT2P	$ 150,245.00	$ 130,713.15
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-5Y-PT2PPP	$ 176,070.00	$ 153,180.90
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-5Y-PT2PP	$ 281,350.00	$ 244,774.50
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-5Y-PT2PP	$ 422,025.00	$ 367,161.75
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-5Y-PT2PP	$ 562,705.00	$ 489,553.35
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-5Y-PT2PP	$ 703,380.00	$ 611,940.60
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-5Y-PT2PP	$ 844,055.00	$ 734,327.85
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-5Y-PT2PP	$ 984,730.00	$ 856,715.10
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-5Y-PT2PP	$ 1,125,405.00	$ 979,102.35
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-1Y-USG2U	$ 5,523.00	$ 4,805.01
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-1Y-USG2	$ 5,949.00	$ 5,175.63
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-1Y-USG2U	$ 6,060.00	$ 5,272.20
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-1Y-USG2	$ 7,407.00	$ 6,444.09
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-1Y-USG2	$ 11,110.00	$ 9,665.70
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-1Y-USG2	$ 13,254.00	$ 11,530.98
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-1Y-USG2	$ 15,739.00	$ 13,692.93
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-1Y-USG2	$ 18,887.00	$ 16,431.69
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-1Y-USG2	$ 22,035.00	$ 19,170.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-1Y-USG2	$ 25,182.00	$ 21,908.34
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-1Y-USG2	$ 28,330.00	$ 24,647.10
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-1Y-USG2	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-1Y-USG2	$ 34,626.00	$ 30,124.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-1Y-USG2	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-1Y-USG2	$ 40,921.00	$ 35,601.27
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-1Y-USG2	$ 44,069.00	$ 38,340.03
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-1Y-USG2	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-1Y-USG2	$ 50,365.00	$ 43,817.55
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-2Y-USG2U	$ 11,046.00	$ 9,610.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-2Y-USG2	$ 11,898.00	$ 10,351.26
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-2Y-USG2U	$ 12,120.00	$ 10,544.40
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-2Y-USG2	$ 14,814.00	$ 12,888.18
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-2Y-USG2	$ 22,220.00	$ 19,331.40
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-2Y-USG2	$ 26,508.00	$ 23,061.96
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-2Y-USG2	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-2Y-USG2	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-2Y-USG2	$ 44,070.00	$ 38,340.90
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-2Y-USG2	$ 50,364.00	$ 43,816.68
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-2Y-USG2	$ 56,660.00	$ 49,294.20
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-2Y-USG2	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-2Y-USG2	$ 69,252.00	$ 60,249.24
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-2Y-USG2	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-2Y-USG2	$ 81,842.00	$ 71,202.54
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-2Y-USG2	$ 88,138.00	$ 76,680.06
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-2Y-USG2	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-2Y-USG2	$ 100,730.00	$ 87,635.10
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-3Y-USG2U	$ 16,569.00	$ 14,415.03
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-3Y-USG2	$ 17,847.00	$ 15,526.89
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-3Y-USG2U	$ 18,180.00	$ 15,816.60
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-3Y-USG2	$ 22,221.00	$ 19,332.27

FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-3Y-USG2	$ 33,330.00	$ 28,997.10
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-3Y-USG2	$ 39,762.00	$ 34,592.94
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-3Y-USG2	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-3Y-USG2	$ 56,661.00	$ 49,295.07
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-3Y-USG2	$ 66,105.00	$ 57,511.35
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-3Y-USG2	$ 75,546.00	$ 65,725.02
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-3Y-USG2	$ 84,990.00	$ 73,941.30
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-3Y-USG2	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-3Y-USG2	$ 103,878.00	$ 90,373.86
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-3Y-USG2	$ 113,322.00	$ 98,590.14
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-3Y-USG2	$ 122,763.00	$ 106,803.81
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-3Y-USG2	$ 132,207.00	$ 115,020.09
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-3Y-USG2	$ 141,651.00	$ 123,236.37
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-3Y-USG2	$ 151,095.00	$ 131,452.65
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-4Y-USG2U	$ 22,092.00	$ 19,220.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-4Y-USG2	$ 23,796.00	$ 20,702.52
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-4Y-USG2U	$ 24,240.00	$ 21,088.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-4Y-USG2	$ 29,628.00	$ 25,776.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-4Y-USG2	$ 44,440.00	$ 38,662.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-4Y-USG2	$ 53,016.00	$ 46,123.92
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-4Y-USG2	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-4Y-USG2	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-4Y-USG2	$ 88,140.00	$ 76,681.80
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-4Y-USG2	$ 100,728.00	$ 87,633.36
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-4Y-USG2	$ 113,320.00	$ 98,588.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-4Y-USG2	$ 125,912.00	$ 109,543.44
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-4Y-USG2	$ 138,504.00	$ 120,498.48
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-4Y-USG2	$ 151,096.00	$ 131,453.52
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-4Y-USG2	$ 163,684.00	$ 142,405.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-4Y-USG2	$ 176,276.00	$ 153,360.12
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-4Y-USG2	$ 188,868.00	$ 164,315.16
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-4Y-USG2	$ 201,460.00	$ 175,270.20
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-5Y-USG2U	$ 27,615.00	$ 24,025.05
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-5Y-USG2	$ 29,745.00	$ 25,878.15
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-5Y-USG2U	$ 30,300.00	$ 26,361.00
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-5Y-USG2	$ 37,035.00	$ 32,220.45
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-5Y-USG2	$ 55,550.00	$ 48,328.50
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-5Y-USG2	$ 66,270.00	$ 57,654.90
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-5Y-USG2	$ 78,695.00	$ 68,464.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-5Y-USG2	$ 94,435.00	$ 82,158.45
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-5Y-USG2	$ 110,175.00	$ 95,852.25
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-5Y-USG2	$ 125,910.00	$ 109,541.70
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-5Y-USG2	$ 141,650.00	$ 123,235.50
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-5Y-USG2	$ 157,390.00	$ 136,929.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-5Y-USG2	$ 173,130.00	$ 150,623.10
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-5Y-USG2	$ 188,870.00	$ 164,316.90
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-5Y-USG2	$ 204,605.00	$ 178,006.35
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-5Y-USG2	$ 220,345.00	$ 191,700.15
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-5Y-USG2	$ 236,085.00	$ 205,393.95

FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-5Y-USG2	$ 251,825.00	$ 219,087.75
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-1Y-USG2U	$ 11,632.00	$ 10,119.84
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-1Y-USG2	$ 13,813.00	$ 12,017.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-1Y-USG2U	$ 15,731.00	$ 13,685.97
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-1Y-USG2	$ 23,798.00	$ 20,704.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-1Y-USG2	$ 35,697.00	$ 31,056.39
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-1Y-USG2	$ 47,597.00	$ 41,409.39
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-1Y-USG2	$ 59,496.00	$ 51,761.52
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-1Y-USG2	$ 71,395.00	$ 62,113.65
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-1Y-USG2	$ 83,294.00	$ 72,465.78
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-1Y-USG2	$ 95,193.00	$ 82,817.91
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-1Y-USG2	$ 107,092.00	$ 93,170.04
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-1Y-USG2	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-1Y-USG2	$ 130,891.00	$ 113,875.17
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-1Y-USG2	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-1Y-USG2	$ 154,689.00	$ 134,579.43
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-1Y-USG2	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-1Y-USG2	$ 178,487.00	$ 155,283.69
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-1Y-USG2	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-2Y-USG2U	$ 23,264.00	$ 20,239.68
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-2Y-USG2	$ 27,626.00	$ 24,034.62
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-2Y-USG2U	$ 31,462.00	$ 27,371.94
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-2Y-USG2	$ 47,596.00	$ 41,408.52
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-2Y-USG2	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-2Y-USG2	$ 95,194.00	$ 82,818.78
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-2Y-USG2	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-2Y-USG2	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-2Y-USG2	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-2Y-USG2	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-2Y-USG2	$ 214,184.00	$ 186,340.08
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-2Y-USG2	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-2Y-USG2	$ 261,782.00	$ 227,750.34
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-2Y-USG2	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-2Y-USG2	$ 309,378.00	$ 269,158.86
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-2Y-USG2	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-2Y-USG2	$ 356,974.00	$ 310,567.38
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-2Y-USG2	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-3Y-USG2U	$ 34,896.00	$ 30,359.52
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-3Y-USG2	$ 41,439.00	$ 36,051.93
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-3Y-USG2U	$ 47,193.00	$ 41,057.91
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-3Y-USG2	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-3Y-USG2	$ 107,091.00	$ 93,169.17
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-3Y-USG2	$ 142,791.00	$ 124,228.17
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-3Y-USG2	$ 178,488.00	$ 155,284.56
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-3Y-USG2	$ 214,185.00	$ 186,340.95
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-3Y-USG2	$ 249,882.00	$ 217,397.34
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-3Y-USG2	$ 285,579.00	$ 248,453.73
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-3Y-USG2	$ 321,276.00	$ 279,510.12
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-3Y-USG2	$ 356,976.00	$ 310,569.12

FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-3Y-USG2	$ 392,673.00	$ 341,625.51
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-3Y-USG2	$ 428,370.00	$ 372,681.90
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-3Y-USG2	$ 464,067.00	$ 403,738.29
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-3Y-USG2	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-3Y-USG2	$ 535,461.00	$ 465,851.07
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-3Y-USG2	$ 571,158.00	$ 496,907.46
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-4Y-USG2U	$ 46,528.00	$ 40,479.36
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-4Y-USG2	$ 55,252.00	$ 48,069.24
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-4Y-USG2U	$ 62,924.00	$ 54,743.88
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-4Y-USG2	$ 95,192.00	$ 82,817.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-4Y-USG2	$ 142,788.00	$ 124,225.56
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-4Y-USG2	$ 190,388.00	$ 165,637.56
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-4Y-USG2	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-4Y-USG2	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-4Y-USG2	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-4Y-USG2	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-4Y-USG2	$ 428,368.00	$ 372,680.16
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-4Y-USG2	$ 475,968.00	$ 414,092.16
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-4Y-USG2	$ 523,564.00	$ 455,500.68
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-4Y-USG2	$ 571,160.00	$ 496,909.20
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-4Y-USG2	$ 618,756.00	$ 538,317.72
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-4Y-USG2	$ 666,352.00	$ 579,726.24
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-4Y-USG2	$ 713,948.00	$ 621,134.76
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-4Y-USG2	$ 761,544.00	$ 662,543.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-5Y-USG2U	$ 58,160.00	$ 50,599.20
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-5Y-USG2	$ 69,065.00	$ 60,086.55
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-5Y-USG2U	$ 78,655.00	$ 68,429.85
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-5Y-USG2	$ 118,990.00	$ 103,521.30
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-5Y-USG2	$ 178,485.00	$ 155,281.95
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-5Y-USG2	$ 237,985.00	$ 207,046.95
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-5Y-USG2	$ 297,480.00	$ 258,807.60
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-5Y-USG2	$ 356,975.00	$ 310,568.25
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-5Y-USG2	$ 416,470.00	$ 362,328.90
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-5Y-USG2	$ 475,965.00	$ 414,089.55
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-5Y-USG2	$ 535,460.00	$ 465,850.20
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-5Y-USG2	$ 594,960.00	$ 517,615.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-5Y-USG2	$ 654,455.00	$ 569,375.85
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-5Y-USG2	$ 713,950.00	$ 621,136.50
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-5Y-USG2	$ 773,445.00	$ 672,897.15
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-5Y-USG2	$ 832,940.00	$ 724,657.80
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-5Y-USG2	$ 892,435.00	$ 776,418.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-5Y-USG2	$ 951,930.00	$ 828,179.10
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-1Y-USG2U	$ 24,621.00	$ 21,420.27
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-1Y-USG2	$ 30,049.00	$ 26,142.63
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-1Y-USG2U	$ 35,214.00	$ 30,636.18
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-1Y-USG2U	$ 56,270.00	$ 48,954.90
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-1Y-USG2U	$ 84,405.00	$ 73,432.35
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-1Y-USG2U	$ 112,541.00	$ 97,910.67
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-1Y-USG2U	$ 140,676.00	$ 122,388.12

FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-1Y-USG2U	$ 168,811.00	$ 146,865.57
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-1Y-USG2U	$ 196,946.00	$ 171,343.02
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-1Y-USG2U	$ 225,081.00	$ 195,820.47
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-2Y-USG2US	$ 49,242.00	$ 42,840.54
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-2Y-USG2	$ 60,098.00	$ 52,285.26
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-2Y-USG2US	$ 70,428.00	$ 61,272.36
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-2Y-USG2U	$ 112,540.00	$ 97,909.80
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-2Y-USG2U	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-2Y-USG2U	$ 225,082.00	$ 195,821.34
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-2Y-USG2U	$ 281,352.00	$ 244,776.24
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-2Y-USG2U	$ 337,622.00	$ 293,731.14
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-2Y-USG2U	$ 393,892.00	$ 342,686.04
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-2Y-USG2U	$ 450,162.00	$ 391,640.94
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-3Y-USG2US	$ 73,863.00	$ 64,260.81
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-3Y-USG2	$ 90,147.00	$ 78,427.89
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-3Y-USG2US	$ 105,642.00	$ 91,908.54
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-3Y-USG2U	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-3Y-USG2U	$ 253,215.00	$ 220,297.05
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-3Y-USG2U	$ 337,623.00	$ 293,732.01
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-3Y-USG2U	$ 422,028.00	$ 367,164.36
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-3Y-USG2U	$ 506,433.00	$ 440,596.71
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-3Y-USG2U	$ 590,838.00	$ 514,029.06
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-3Y-USG2U	$ 675,243.00	$ 587,461.41
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-4Y-USG2US	$ 98,484.00	$ 85,681.08
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-4Y-USG2	$ 120,196.00	$ 104,570.52
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-4Y-USG2US	$ 140,856.00	$ 122,544.72
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-4Y-USG2U	$ 225,080.00	$ 195,819.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-4Y-USG2U	$ 337,620.00	$ 293,729.40
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-4Y-USG2U	$ 450,164.00	$ 391,642.68
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-4Y-USG2U	$ 562,704.00	$ 489,552.48
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-4Y-USG2U	$ 675,244.00	$ 587,462.28
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-4Y-USG2U	$ 787,784.00	$ 685,372.08
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-4Y-USG2U	$ 900,324.00	$ 783,281.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-5Y-USG2US	$ 123,105.00	$ 107,101.35
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-5Y-USG2	$ 150,245.00	$ 130,713.15
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-5Y-USG2US	$ 176,070.00	$ 153,180.90
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-5Y-USG2U	$ 281,350.00	$ 244,774.50
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-5Y-USG2U	$ 422,025.00	$ 367,161.75
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-5Y-USG2U	$ 562,705.00	$ 489,553.35
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-5Y-USG2U	$ 703,380.00	$ 611,940.60
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-5Y-USG2U	$ 844,055.00	$ 734,327.85
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-5Y-USG2U	$ 984,730.00	$ 856,715.10
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-5Y-USG2U	$ 1,125,405.00	$ 979,102.35
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 500-999	RN-MC-MSMC-000999-1Y	$ 52.00	$ 45.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 500-999	RN-MC-MSMC-000999-2Y	$ 104.00	$ 90.48
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 500-999	RN-MC-MSMC-000999-3Y	$ 140.40	$ 122.15
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 500-999	RN-MC-MSMC-000999-4Y	$ 187.20	$ 162.86
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 1000-1999	RN-MC-MSMC-001999-1Y	$ 43.00	$ 37.41
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 1000-1999	RN-MC-MSMC-001999-2Y	$ 86.00	$ 74.82

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 1000-1999	RN-MC-MSMC-001999-3Y	$ 116.10	$ 101.01
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 1000-1999	RN-MC-MSMC-001999-4Y	$ 154.80	$ 134.68
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 2000-4999	RN-MC-MSMC-004999-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 2000-4999	RN-MC-MSMC-004999-2Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 2000-4999	RN-MC-MSMC-004999-3Y	$ 97.20	$ 84.56
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 2000-4999	RN-MC-MSMC-004999-4Y	$ 129.60	$ 112.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 5000-9999	RN-MC-MSMC-009999-1Y	$ 30.00	$ 26.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 5000-9999	RN-MC-MSMC-009999-2Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 5000-9999	RN-MC-MSMC-009999-3Y	$ 81.00	$ 70.47
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 5000-9999	RN-MC-MSMC-009999-4Y	$ 108.00	$ 93.96
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 10000-19999	RN-MC-MSMC-019999-1Y	$ 25.00	$ 21.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 10000-19999	RN-MC-MSMC-019999-2Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 10000-19999	RN-MC-MSMC-019999-3Y	$ 67.50	$ 58.73
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 10000-19999	RN-MC-MSMC-019999-4Y	$ 90.00	$ 78.30
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 20000-49999	RN-MC-MSMC-049999-1Y	$ 21.00	$ 18.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 20000-49999	RN-MC-MSMC-049999-2Y	$ 42.00	$ 36.54
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 20000-49999	RN-MC-MSMC-049999-3Y	$ 56.70	$ 49.33
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 20000-49999	RN-MC-MSMC-049999-4Y	$ 75.60	$ 65.77
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 50000-74999	RN-MC-MSMC-074999-1Y	$ 17.00	$ 14.79
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 50000-74999	RN-MC-MSMC-074999-2Y	$ 34.00	$ 29.58
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 50000-74999	RN-MC-MSMC-074999-3Y	$ 45.90	$ 39.93
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 50000-74999	RN-MC-MSMC-074999-4Y	$ 61.20	$ 53.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 75000-99999	RN-MC-MSMC-099999-1Y	$ 14.00	$ 12.18
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 75000-99999	RN-MC-MSMC-099999-2Y	$ 28.00	$ 24.36
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 75000-99999	RN-MC-MSMC-099999-3Y	$ 37.80	$ 32.89
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 75000-99999	RN-MC-MSMC-099999-4Y	$ 50.40	$ 43.85
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100000+	RN-MC-MSMC-100000+1Y	$ 12.00	$ 10.44
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100000+	RN-MC-MSMC-100000+2Y	$ 24.00	$ 20.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100000+	RN-MC-MSMC-100000+3Y	$ 32.40	$ 28.19
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100000+	RN-MC-MSMC-100000+4Y	$ 43.20	$ 37.58
FireEye	MX 900 Appliance Cold Standby- Mobile Threat Prevention - Mobile Security Management	900MX-HWCOLDSB	$ 7,995.00	$ 6,955.65
FireEye	MX 8400 Appliance/Server Cold Standby- Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HWCOLDSB	$ 64,995.00	$ 56,545.65
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - Platinum-PROMOTION	TAP-1KEPS-SS-3M-P	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - Plat Prio Plus-PROMOTION	TAP-1KEPS-SS-3M-PPP	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - GovUS-PROMOTION	TAP-1KEPS-SS-3M-US	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - GovUS Prio Plus-PROMOTION	TAP-1KEPS-SS-3M-USPP	$ -	$ -
Google	Google Apps for Business: 12 month license/support term; 1 seat;	GAPPS-PREM-1USER-12MO	$ 50.00	$ 48.87
Google	Google Apps for Business Upgrade: 1 month license/support term; 1 seat;	GAPPS-PREM-UPG-1USER-1M	$ 4.17	$ 4.08
Google	Google Apps Vault: 12 month license/support term; 1 seat;	GAPPS-VAULT-1USER-12MO	$ 50.00	$ 48.87
Google	Google Apps Vault Upgrade: 1 month license/support term; 1 seat;	GAPPS-VAULT-UPG-1USER-1	$ 4.17	$ 4.08
Google	Google Apps Unlimited: 12 month license/support term; 1 seat;	GAPPS-UNLIM-1-USER-12-M	$ 120.00	$ 117.28
Google	Google Apps Unlimited Upgrade: 1 month license/support term; 1 seat;	GAPPS-UNLIM-1-USER-1-MO	$ 10.00	$ 9.77
Google	Google Apps Message Encryption: 12 month license/support term; 1 seat;	GAPPS-ME-WITHCOMPOSE-1	$ 35.00	$ 34.21
Google	Google Apps Message Encryption Upgrade: 1 month license/support term; 1 seat;	GAPPS-ME-CUSTPRTL-1USER	$ 2.92	$ 2.85
QTS	SOC Reports type II Bundle - Gold NRR	10800100011-000	$ 500.00	$ 488.66
QTS	SOC Reports type II Bundle - Gold MRR	10811100011-000	$ 340.00	$ 332.29
QTS	Security Engineer T&M MRC MRR	10811100016-000	$ 170.00	$ 166.15
QTS	Licensing Services Early Term Fee NRR	11200100003-000	$ 1,010.00	$ 987.10
QTS	Licensing Service Cancellation Fee NRR	11200100004-000	$ 10,100.00	$ 9,871.03

QTS	NetBackup for SQL Server - Tier 1: Single Processor One Time Charge NRR	11200NET00013-000	$ 1,618.75	$ 1,582.05
QTS	Connectivity: MetroConnect Protected 10 Gbps NRR	11400000041-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: IP Bandwith Copper - Setup Fee NRR	11400100001-000	$ 500.00	$ 488.66
QTS	Connectivity: IP Bandwith Fiber - Setup Fee NRR	11400100002-000	$ 1,000.00	$ 977.33
QTS	Connectivity: Copper Cross Connect NRR	11400100003-000	$ 500.00	$ 488.66
QTS	Connectivity: T1 NRR	11400100003-0T1	$ 100.00	$ 97.73
QTS	Connectivity: AT&T Copper Cross Connect NRR	11400100003-ATT	$ 500.00	$ 488.66
QTS	Connectivity: Verizon Business Copper Cross Connect NRR	11400100003-VZB	$ 500.00	$ 488.66
QTS	Connectivity: Verizon Copper Cross Connect NRR	11400100003-VZN	$ 500.00	$ 488.66
QTS	Connectivity: Copper Cross Connect (Home Run) NRR	11400100004-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: Fiber Cross Connect NRR	11400100005-000	$ 1,000.00	$ 977.33
QTS	Connectivity: AT&T Fiber Cross Connect NRR	11400100005-ATT	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Business Fiber Cross Connect NRR	11400100005-VZB	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Fiber Cross Connect NRR	11400100005-VZN	$ 1,000.00	$ 977.33
QTS	Connectivity: Fiber Cross Connect (Home Run) NRR	11400100006-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 1 Gbps NRR	11400100027-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Standard 1 Gbps NRR	11400100027-RIC	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 10 Gbps NRR	11400100028-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: MetroConnect Standard 10 Gbps NRR	11400100028-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: MetroConnect Standard 100 Mbps NRR	11400100034-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: POTS NRR	11400100035-000	$ 100.00	$ 97.73
QTS	Connectivity: MetroConnect Protected 100 Mbps NRR	11400100039-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Protected 1 Gbps NRR	11400100040-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Protected 1 Gbps NRR	11400100040-RIC	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Protected 10 Gbps NRR	11400100041-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: Data Center Connect 10MB - Atlanta NRR	11400100045-ATL	$ 300.00	$ 293.20
QTS	Connectivity: Data Center Connect 10MB - Richmond NRR	11400100053-RIC	$ 300.00	$ 293.20
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Atlanta NRR	11400100058-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Richmond NRR	11400100060-RIC	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Atlanta NRR	11400100064-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Richmond NRR	11400100066-RIC	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Atlanta NRR	11400100070-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Richmond NRR	11400100072-RIC	$ 100.00	$ 97.73
QTS	Connectivity: AT&T Coax Cross Connect NRR	11400100073-ATT	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Coax Cross Connect NRR	11400100074-VZN	$ 1,000.00	$ 977.33
QTS	Connectivity: Coax Cross Connect NRR	11400100075-000	$ 1,000.00	$ 977.33
QTS	Connectivity: Copper Cross Connect MRR	11411100021-000	$ 150.00	$ 146.60
QTS	Connectivity: T1 MRR	11411100021-0T1	$ 25.00	$ 24.43
QTS	Connectivity: AT&T Copper Cross Connect MRR	11411100021-ATT	$ 200.00	$ 195.47
QTS	Connectivity: Verizon Business Copper Cross Connect MRR	11411100021-VZB	$ 200.00	$ 195.47
QTS	Connectivity: Verizon Copper Cross Connect MRR	11411100021-VZN	$ 200.00	$ 195.47
QTS	Connectivity: Copper Cross Connect (Home Run) MRR	11411100022-000	$ 5,800.00	$ 5,668.51
QTS	Connectivity: Fiber Cross Connect MRR	11411100023-000	$ 300.00	$ 293.20
QTS	Connectivity: AT&T Fiber Cross Connect MRR	11411100023-ATT	$ 350.00	$ 342.07
QTS	Connectivity: Verizon Business Fiber Cross Connect MRR	11411100023-VNB	$ 350.00	$ 342.07
QTS	Connectivity: Verizon Fiber Cross Connect MRR	11411100023-VZN	$ 350.00	$ 342.07
QTS	Connectivity: Fiber Cross Connect (Home Run) MRR	11411100024-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 1 Gbps MRR	11411100027-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Standard 1 Gbps MRR	11411100027-RIC	$ 4,500.00	$ 4,397.98

QTS	Connectivity: MetroConnect Standard 10 Gbps MRR	11411100028-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: MetroConnect Standard 10 Gbps MRR	11411100028-RIC	$ 8,500.00	$ 8,307.30
QTS	IP Bandwidth - 1 Gbps port - (1-4 Mbps Commit) MRR	11411100032-G04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 1 Gbps port - (5-9 Mbps Commit) MRR	11411100032-G09	$ 75.00	$ 73.30
QTS	IP Bandwidth - 1 Gbps port - (10-19 Mbps Commit) MRR	11411100032-G19	$ 60.00	$ 58.64
QTS	IP Bandwidth - 1 Gbps port - (500-1000 Mbps Commit) MRR	11411100032-G1G	$ 8.00	$ 7.82
QTS	IP Bandwidth - 1 Gbps port - (100-199 Mbps Commit) MRR	11411100032-G1H	$ 30.00	$ 29.32
QTS	IP Bandwidth - 1 Gbps port - (200-299 Mbps Commit) MRR	11411100032-G2H	$ 25.00	$ 24.43
QTS	IP Bandwidth - 1 Gbps port - (300-399 Mbps Commit) MRR	11411100032-G3H	$ 20.00	$ 19.55
QTS	Space Services - Cage NRR	10000100001-000	$ 48.00	$ 46.91
QTS	Space Services - Cabinet NRR	10000100004-000	$ 975.00	$ 952.90
QTS	Space: Cubicle Space NRR	10000100006-000	$ 100.00	$ 97.73
QTS	Space: Customer Provided Rack Install - One Time Fee NRR	10000100027-000	$ 250.00	$ 244.33
QTS	Space: Rack - (4 Post) NRR	10000100030-000	$ 80.00	$ 78.19
QTS	Space: Rack - (2 Post) NRR	10000100033-000	$ 80.00	$ 78.19
QTS	Space Services: High Density Cabinet 8 kW NRR	10000100056-000	$ 1,500.00	$ 1,465.99
QTS	Space Services: High Density Cabinet 16 kW NRR	10000100057-000	$ 3,600.00	$ 3,518.39
QTS	Space Services: High Density Cage 24 kW NRR	10000100058-000	$ 160.00	$ 156.37
QTS	Space Services: High Density Cage 36 kW + NRR	10000100059-000	$ 160.00	$ 156.37
QTS	Space Services: 3300 sq. ft. Suite - Richmond NRR	10000100066-RIC	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Metro NRR	10000100067-ATL	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Suwanee NRR	10000100068-SUW	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Dallas NRR	10000100069-DFW	$ 80,000.00	$ 78,186.40
QTS	Space Services - Cage MRR	10011100001-000	$ 22.00	$ 21.50
QTS	Space Services - Cabinet MRR	10011100004-000	$ 635.00	$ 620.60
QTS	Space Services - Suite MRR	10011100008-000	$ 30.00	$ 29.32
QTS	Space: Rack - (4 Post) MRR	10011100030-000	$ 40.00	$ 39.09
QTS	Space: Rack - (2 Post) MRR	10011100033-000	$ 40.00	$ 39.09
QTS	Space Services: High Density Cabinet 8 kW MRR	10011100056-000	$ 1,150.00	$ 1,123.93
QTS	Space Services: High Density Cabinet 16 kW MRR	10011100057-000	$ 2,150.00	$ 2,101.26
QTS	Space Services: High Density Cage 24 kW MRR	10011100058-000	$ 40.00	$ 39.09
QTS	Space Services: High Density Cage 36 kW + MRR	10011100059-000	$ 70.00	$ 68.41
QTS	Power 120V 20Amp Primary NRR	10200100001-000	$ 600.00	$ 586.40
QTS	Power 120V 20Amp Primary NRR	10200100001-NYC	$ 1,560.00	$ 1,524.63
QTS	Power 120V 20Amp Redundant NRR	10200100002-000	$ 600.00	$ 586.40
QTS	IP Bandwidth - 1 Gbps port - (20-49 Mbps Commit) MRR	11411100032-G49	$ 50.00	$ 48.87
QTS	IP Bandwidth - 1 Gbps port - (400-499 Mbps Commit) MRR	11411100032-G4H	$ 12.00	$ 11.73
QTS	IP Bandwidth - 1 Gbps port - (50-99 Mbps Commit) MRR	11411100032-G99	$ 40.00	$ 39.09
QTS	IP Bandwidth - 100 Mbps port - (1-4 Mbps Commit) MRR	11411100032-H04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 100 Mbps port - (5-9 Mbps Commit) MRR	11411100032-H09	$ 75.00	$ 73.30
QTS	IP Bandwidth - 100 Mbps port - (10-19 Mbps Commit) MRR	11411100032-H19	$ 60.00	$ 58.64
QTS	IP Bandwidth - 100 Mbps port - (50-100 Mbps Commit) MRR	11411100032-H1H	$ 40.00	$ 39.09
QTS	IP Bandwidth - 100 Mbps port - (20-49 Mbps Commit) MRR	11411100032-H49	$ 50.00	$ 48.87
QTS	IP Bandwidth - 10 Mbps port - (1-4 Mbps Commit) MRR	11411100032-T04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 10 Mbps port - (5-10 Mbps Commit) MRR	11411100032-T10	$ 75.00	$ 73.30
QTS	Connectivity: MetroConnect Standard 100 Mbps MRR	11411100034-ATL	$ 500.00	$ 488.66
QTS	Connectivity: POTS MRR	11411100035-000	$ 25.00	$ 24.43
QTS	Connectivity: MetroConnect Protected 100 Mbps MRR	11411100039-ATL	$ 750.00	$ 733.00
QTS	Connectivity: MetroConnect Protected 1 Gbps MRR	11411100040-ATL	$ 1,500.00	$ 1,465.99

QTS	Connectivity: MetroConnect Protected 1 Gbps MRR	11411100040-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: MetroConnect Protected 10 Gbps MRR	11411100041-ATL	$ 7,500.00	$ 7,329.97
QTS	Connectivity: MetroConnect Protected 10 Gbps MRR	11411100041-RIC	$ 18,000.00	$ 17,591.94
QTS	Connectivity: Data Center Connect 10MB - Atlanta MRR	11411100045-ATL	$ 280.00	$ 273.65
QTS	Connectivity: Data Center Connect 10MB - Richmond MRR	11411100053-RIC	$ 280.00	$ 273.65
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Atlanta MRR	11411100058-ATL	$ 75.00	$ 73.30
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Richmond MRR	11411100060-RIC	$ 75.00	$ 73.30
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Atlanta MRR	11411100064-ATL	$ 60.00	$ 58.64
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Richmond MRR	11411100066-RIC	$ 60.00	$ 58.64
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Atlanta MRR	11411100070-ATL	$ 50.00	$ 48.87
QTS	Power 120V 20Amp Redundant NRR	10200100002-NYC	$ 1,560.00	$ 1,524.63
QTS	Power 120V 30Amp Primary NRR	10200100003-000	$ 600.00	$ 586.40
QTS	Power 120V 30Amp Primary NRR	10200100003-NYC	$ 1,690.00	$ 1,651.69
QTS	Power 120V 30Amp Redundant NRR	10200100004-000	$ 600.00	$ 586.40
QTS	Power 120V 30Amp Redundant NRR	10200100004-NYC	$ 1,690.00	$ 1,651.69
QTS	Power 208v 20Amp Primary NRR	10200100006-000	$ 600.00	$ 586.40
QTS	Power 208v 20Amp Redundant NRR	10200100007-000	$ 600.00	$ 586.40
QTS	Power 208v 30Amp Primary NRR	10200100008-000	$ 600.00	$ 586.40
QTS	Power 208v 30Amp Redundant NRR	10200100009-000	$ 600.00	$ 586.40
QTS	Power 208v 50Amp Primary NRR	10200100010-000	$ 600.00	$ 586.40
QTS	Power 208v 50Amp Redundant NRR	10200100011-000	$ 600.00	$ 586.40
QTS	Power 208v 60Amp Primary NRR	10200100012-000	$ 600.00	$ 586.40
QTS	Power 208v 60Amp Redundant NRR	10200100013-000	$ 600.00	$ 586.40
QTS	Power 3 Phase 208v 20Amp Primary NRR	10200100014-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 20Amp Redundant NRR	10200100015-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Primary NRR	10200100016-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Primary NRR	10200100016-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 30Amp Redundant NRR	10200100017-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Redundant NRR	10200100017-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 50Amp Primary NRR	10200100018-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 50Amp Primary NRR	10200100018-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 50Amp Redundant NRR	10200100019-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 50Amp Redundant NRR	10200100019-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 60Amp Primary NRR	10200100020-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 60Amp Primary NRR	10200100020-JCY	$ 2,000.00	$ 1,954.66
QTS	Power 3 Phase 208v 60Amp Redundant NRR	10200100021-000	$ 1,400.00	$ 1,368.26
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Richmond MRR	11411100072-RIC	$ 50.00	$ 48.87
QTS	Connectivity: AT&T Coax Cross Connect MRR	11411100073-ATT	$ 250.00	$ 244.33
QTS	Connectivity: Verizon Coax Cross Connect MRR	11411100074-VZN	$ 300.00	$ 293.20
QTS	Connectivity: Coax Cross Connect MRR	11411100075-000	$ 300.00	$ 293.20
QTS	Federal Cloud - DR - Internet Overage MRR	11500000089-000	$ 30.00	$ 29.32
QTS	Federal Cloud - VPU 1 Ghz MRR	11500000097-000	$ 40.00	$ 39.09
QTS	Federal Cloud - RAM 1 GB MRR	11500000098-000	$ 32.00	$ 31.27
QTS	Federal Cloud - Bronze Storage 1GB MRR	11500000099-000	$ 0.41	$ 0.40
QTS	Federal Cloud - Silver Storage 1GB MRR	11500000100-000	$ 0.53	$ 0.52
QTS	Federal Cloud - Gold Storage 1GB MRR	11500000101-000	$ 1.65	$ 1.61
QTS	Federal Cloud - Large Firewall MRR	11500000102-000	$ 225.00	$ 219.90
QTS	Federal Cloud - Internet 1Mbps MRR	11500000103-000	$ 20.00	$ 19.55
QTS	Federal Cloud - Internet Overage MRR	11500000104-000	$ 30.00	$ 29.32

QTS	Federal Cloud - Additional Public IP MRR	11500000105-000	$ 15.00	$ 14.66
QTS	Federal Cloud - Additional Network Segments MRR	11500000106-000	$ 50.00	$ 48.87
QTS	Federal Cloud - Client to Site VPN (Qty 5) MRR	11500000107-000	$ 5.00	$ 4.89
QTS	Federal Cloud - DR - VPU 1Ghz MRR	11500000113-000	$ 23.00	$ 22.48
QTS	Federal Cloud - DR - RAM 1 GB MRR	11500000114-000	$ 19.00	$ 18.57
QTS	Federal Cloud - DR - Bronze Storage 1GB MRR	11500000115-000	$ 0.24	$ 0.23
QTS	Federal Cloud - DR - Silver Storage 1GB MRR	11500000116-000	$ 0.30	$ 0.29
QTS	Federal Cloud - DR -Gold Storage 1GB MRR	11500000117-000	$ 1.23	$ 1.20
QTS	Federal Cloud - DR - Large Firewall MRR	11500000118-000	$ 225.00	$ 219.90
QTS	Federal Cloud - DR - Internet 1Mbps MRR	11500000119-000	$ 20.00	$ 19.55
QTS	Federal Cloud - DR -Additional Public IP MRR	11500000121-000	$ 7.50	$ 7.33
QTS	Federal Cloud - DR - Additional Network Segments MRR	11500000122-000	$ 25.00	$ 24.43
QTS	Power 3 Phase 208v 60Amp Redundant NRR	10200100021-JCY	$ 2,000.00	$ 1,954.66
QTS	Power 120V 20Amp Primary MRR	10211100001-000	$ 360.00	$ 351.84
QTS	Power 120V 20Amp Primary MRR	10211100001-NYC	$ 450.00	$ 439.80
QTS	Power 120V 20Amp Redundant MRR	10211100002-000	$ 90.00	$ 87.96
QTS	Power 120V 20Amp Redundant MRR	10211100002-NYC	$ 225.00	$ 219.90
QTS	Power 120V 30Amp Primary MRR	10211100003-000	$ 520.00	$ 508.21
QTS	Power 120V 30Amp Primary MRR	10211100003-NYC	$ 680.00	$ 664.58
QTS	Power 120V 30Amp Redundant MRR	10211100004-000	$ 130.00	$ 127.05
QTS	Power 120V 30Amp Redundant MRR	10211100004-NYC	$ 340.00	$ 332.29
QTS	Power 208v 20Amp Primary MRR	10211100006-000	$ 600.00	$ 586.40
QTS	Power 208v 20Amp Redundant MRR	10211100007-000	$ 150.00	$ 146.60
QTS	Power 208v 30Amp Primary MRR	10211100008-000	$ 900.00	$ 879.60
QTS	Power 208v 30Amp Redundant MRR	10211100009-000	$ 225.00	$ 219.90
QTS	Power 208v 50Amp Primary MRR	10211100010-000	$ 1,540.00	$ 1,505.09
QTS	Power 208v 50Amp Redundant MRR	10211100011-000	$ 385.00	$ 376.27
QTS	Power 208v 60Amp Primary MRR	10211100012-000	$ 1,760.00	$ 1,720.10
QTS	Power 208v 60Amp Redundant MRR	10211100013-000	$ 440.00	$ 430.03
QTS	Power 3 Phase 208v 20Amp Primary MRR	10211100014-000	$ 1,000.00	$ 977.33
QTS	Power 3 Phase 208v 20Amp Redundant MRR	10211100015-000	$ 250.00	$ 244.33
QTS	Power 3 Phase 208v 30Amp Primary MRR	10211100016-000	$ 1,500.00	$ 1,465.99
QTS	Power 3 Phase 208v 30Amp Primary MRR	10211100016-JCY	$ 2,900.00	$ 2,834.26
QTS	Power 3 Phase 208v 30Amp Redundant MRR	10211100017-000	$ 375.00	$ 366.50
QTS	Power 3 Phase 208v 30Amp Redundant MRR	10211100017-JCY	$ 375.00	$ 366.50
QTS	Power 3 Phase 208v 50Amp Primary MRR	10211100018-000	$ 2,500.00	$ 2,443.32
QTS	Power 3 Phase 208v 50Amp Primary MRR	10211100018-JCY	$ 4,840.00	$ 4,730.28
QTS	Power 3 Phase 208v 50Amp Redundant MRR	10211100019-000	$ 625.00	$ 610.83
QTS	Power 3 Phase 208v 50Amp Redundant MRR	10211100019-JCY	$ 1,210.00	$ 1,182.57
QTS	Power 3 Phase 208v 60Amp Primary MRR	10211100020-000	$ 3,040.00	$ 2,971.08
QTS	Power 3 Phase 208v 60Amp Primary MRR	10211100020-JCY	$ 5,800.00	$ 5,668.51
QTS	Power 3 Phase 208v 60Amp Redundant MRR	10211100021-000	$ 760.00	$ 742.77
QTS	Power 3 Phase 208v 60Amp Redundant MRR	10211100021-JCY	$ 1,450.00	$ 1,417.13
QTS	Power: 500kW - N+1 Configuration - Richmond MRR	10211100102-RIC	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Metro MRR	10211100103-ATL	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Suwanee MRR	10211100104-SUW	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Dallas MRR	10211100105-DFW	$ 80,000.00	$ 78,186.40
QTS	Other Custom Data Center Services NRR	10300100034-000	$ 1.00	$ 0.98
QTS	Other Custom Data Center Services MRR	10311100033-000	$ 1.00	$ 0.98

QTS	DBA/Application Developer MRC NRR	10600100001-000	$ 220.00	$ 215.01
QTS	SQL Base Support NRR	10600100005-000	$ 500.00	$ 488.66
QTS	SQL Base Support Cluster NRR	10600100007-000	$ 1,000.00	$ 977.33
QTS	SQL Engineering T&M NRR	10600100008-000	$ 200.00	$ 195.47
QTS	Application Early Termination Fee NRR	10600100020-000	$ 10,100.00	$ 9,871.03
QTS	Application Service Cancellation Fee NRR	10600100021-000	$ 10,100.00	$ 9,871.03
QTS	SQL Base Support MRR	10611100005-000	$ 1,650.00	$ 1,612.59
QTS	SQL Base Support Cluster MRR	10611100006-000	$ 2,500.00	$ 2,443.32
QTS	SQL Engineering T&M MRR	10611100008-000	$ 200.00	$ 195.47
QTS	DBA/Application Developer MRC MRR	10611100020-000	$ 220.00	$ 215.01
QTS	Basic Monitoring - Unmanaged NRR	10700100001-000	$ 33.84	$ 33.07
QTS	Basic Monitoring -Managed NRR	10700100002-000	$ 33.84	$ 33.07
QTS	Enhanced Monitoring - Unmanaged NRR	10700100003-000	$ 42.30	$ 41.34
QTS	Enhanced Monitoring - Managed NRR	10700100004-000	$ 42.30	$ 41.34
QTS	Advanced Monitoring - Unmanaged NRR	10700100005-000	$ 67.68	$ 66.15
QTS	Enterprise Cloud - Back-up services GB Transferred MRR	11511000093-000	$ 0.18	$ 0.18
QTS	Enterprise Cloud - Back-up services GB Usage MRR	11511000120-000	$ 0.18	$ 0.18
QTS	QVI Backup MRR	11511000039-000	$ 0.20	$ 0.20
QTS	Enterprise Cloud - DR - Bronze Storage 1GB MRR	11511000084-000	$ 0.22	$ 0.22
QTS	DRaaS - Bronze Storage 1GB MRR	11511000145-000	$ 0.22	$ 0.22
QTS	Enterprise Cloud - DR - Silver Storage 1GB MRR	11511000085-000	$ 0.26	$ 0.26
QTS	DRaaS - Silver Storage 1GB MRR	11511000146-000	$ 0.26	$ 0.26
QTS	Enterprise Cloud - Bronze Storage 1GB MRR	11511000068-000	$ 0.33	$ 0.33
QTS	DRaaS - EC Reservation - Bronze Storage 1GB MRR	11511000156-000	$ 0.33	$ 0.33
QTS	DR-SAN Disk Capacity GBs MRR	11511000050-000	$ 0.35	$ 0.35
QTS	Enterprise Cloud - Silver Storage 1GB MRR	11511000069-000	$ 0.41	$ 0.41
QTS	DRaaS - EC Reservation - Silver Storage 1GB MRR	11511000157-000	$ 0.41	$ 0.41
QTS	QVI Additional SAN Storage MRR	11511000020-000	$ 0.41	$ 0.41
QTS	QVI Backup Overage MRR	11500000040-000	$ 0.50	$ 0.50
QTS	QVI Infrastructure Improvement Credit (GSA) MRR	11511000169-000	$ 1.00	$ 0.99
QTS	System Services Custom MRR	10511100014-000	$ 1.00	$ 0.99
QTS	Storage Services Custom MRR	11011100031-000	$ 1.00	$ 0.99
QTS	Licensing Services Custom MRR	11211100001-000	$ 1.00	$ 0.99
QTS	Security Services Custom MRR	10811100013-000	$ 1.00	$ 0.99
QTS	System Services Custom NRR	10500100014-000	$ 1.00	$ 0.99
QTS	Security Services Custom NRR	10800100013-000	$ 1.00	$ 0.99
QTS	Storage Services Custom NRR	11000100039-000	$ 1.00	$ 0.99
QTS	Licensing Services Custom NRR	11200100001-000	$ 1.00	$ 0.99
QTS	QVI Infrastructure Improvement Credit (GSA) NRR	11500000169-000	$ 1.00	$ 0.99
QTS	Additional QVI IP addresses MRR	11511000012-000	$ 1.00	$ 0.99
QTS	Enterprise Cloud - DR -Gold Storage 1GB MRR	11511000086-000	$ 1.03	$ 1.02
QTS	DRaaS - Gold Storage 1GB MRR	11511000147-000	$ 1.03	$ 1.02
QTS	Enterprise Cloud - Gold Storage 1GB MRR	11511000070-000	$ 1.44	$ 1.42
QTS	DRaaS - EC Reservation - Gold Storage 1GB MRR	11511000158-000	$ 1.44	$ 1.42
QTS	Enterprise Cloud- Client to Site VPN (Qty 5) MRR	11511000076-000	$ 4.95	$ 4.85
QTS	Enterprise Cloud - DR- Client to Site VPN (Qty 5) MRR	11511000092-000	$ 4.95	$ 4.85
QTS	DRaaS - Client to Site VPN (Qty 5) MRR	11511000153-000	$ 4.95	$ 4.85
QTS	DRaaS - EC Reservation - Client to Site VPN (Qty 5) MRR	11511000164-000	$ 4.95	$ 4.85
QTS	Additional remote clients for VPN Sessions MRR	11511000014-000	$ 6.50	$ 6.36

QTS	Enterprise Cloud - DR -Additional Public IP MRR	11511000090-000	$ 7.50	$ 7.34
QTS	DRaaS - Additional Public IP MRR	11511000151-000	$ 7.50	$ 7.34
QTS	QVI per port cost (3 Ports are required per physical server) MRR	11511000008-000	$ 12.00	$ 11.73
QTS	Enterprise Cloud - DR - RAM 1 GB MRR	11511000083-000	$ 13.00	$ 12.71
QTS	DRaaS - RAM 1 GB MRR	11511000144-000	$ 13.00	$ 12.71
QTS	Enterprise Cloud - Additional Public IP MRR	11511000074-000	$ 15.00	$ 14.66
QTS	DRaaS - EC Reservation - Additional Public IP MRR	11511000162-000	$ 15.00	$ 14.66
QTS	Enterprise Cloud - DR - VPU 1Ghz MRR	11511000082-000	$ 16.00	$ 15.64
QTS	DRaaS - VPU 1Ghz MRR	11511000143-000	$ 16.00	$ 15.64
QTS	Enterprise Cloud - Internet 1Mbps MRR	11511000072-000	$ 18.00	$ 17.59
QTS	Enterprise Cloud - DR - Internet 1Mbps MRR	11511000088-000	$ 18.00	$ 17.59
QTS	DRaaS - Internet 1Mbps MRR	11511000149-000	$ 18.00	$ 17.59
QTS	DRaaS - EC Reservation - Internet 1Mbps MRR	11511000160-000	$ 18.00	$ 17.59
QTS	Additional IP Bandwidth - QVI MRR	11511000007-000	$ 18.00	$ 17.59
QTS	QVI Additional VM VPU MRR	11511000016-000	$ 21.00	$ 20.52
QTS	DRaaS - EC Reservation - RAM 1 GB MRR	11511000155-000	$ 22.75	$ 22.23
QTS	Enterprise Cloud - RAM 1 GB MRR	11511000067-000	$ 23.00	$ 22.48
QTS	Enterprise Cloud - DR - Additional Network Segments MRR	11511000091-000	$ 25.00	$ 24.43
QTS	DRaaS - Additional Network Segments MRR	11511000152-000	$ 25.00	$ 24.43
QTS	QVI Additional VM RAM MRR	11511000017-000	$ 25.00	$ 24.43
QTS	QVI - Windows Standard MRR	11511000023-000	$ 25.00	$ 24.43
QTS	Enterprise Cloud - Internet Overage MRR	11500000073-000	$ 27.00	$ 26.39
QTS	Enterprise Cloud - DR - Internet Overage MRR	11511000120-001	$ 27.00	$ 26.39
QTS	Enterprise Cloud - VPU 1 Ghz MRR	11511000066-000	$ 27.00	$ 26.39
QTS	DRaaS - Internet Overage MRR	11511000150-000	$ 27.00	$ 26.39
QTS	DRaaS - EC Reservation - VPU 1Ghz MRR	11511000154-000	$ 27.00	$ 26.39
QTS	DRaaS - EC Reservation - Internet Overage MRR	11511000161-000	$ 27.00	$ 26.39
QTS	IP Bandwidth - Bursting Overage - QVI MRR	11411100013-000	$ 27.00	$ 26.39
QTS	Additional Site-To-Site VPN Connection NRR	11500000013-000	$ 30.00	$ 29.32
QTS	Additional remote clients for VPN Sessions NRR	11500000014-000	$ 30.00	$ 29.32
QTS	QVI Active Directory for Windows clustering NRR	11500000028-000	$ 35.00	$ 34.21
QTS	Enterprise Cloud - Cloud Network Port MRR	11511000134-000	$ 35.00	$ 34.21
QTS	Enterprise Cloud - Additional Network Segments MRR	11511000075-000	$ 50.00	$ 48.87
QTS	DRaaS - EC Reservation - Additional Network Segments MRR	11511000163-000	$ 50.00	$ 48.87
QTS	QVI - RedHat Advanced / Enterprise per VM MRR	11511000023-002	$ 55.00	$ 53.75
QTS	Virtual Load Balancing NRR	11500000009-000	$ 60.00	$ 58.64
QTS	QVI Additional VM VPU NRR	11500000016-000	$ 60.00	$ 58.64
QTS	QVI Additional VM RAM NRR	11500000017-000	$ 60.00	$ 58.64
QTS	QVI Network - Pair of redundant virtual Firewalls 1 Site to Site VPN or 5 client to Site 1 Meg of Bandwidth NRR	11500000038-000	$ 60.00	$ 58.64
QTS	DR-VM Additional RAM GBs NRR	11500000048-000	$ 60.00	$ 58.64
QTS	DR-VM Additional VPU NRR	11500000049-000	$ 60.00	$ 58.64
QTS	DRaaS - Replication Service per VM MRR	11511000141-000	$ 60.00	$ 58.64
QTS	Optional Space and Power - 110 20amp Power and 1U rack space. MRR	11511000006-000	$ 65.00	$ 63.53
QTS	DR-HA VM with Replication NRR	11500000055-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Standard-Linux NRR	11500000056-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Enterprise NRR	11500000057-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Data Center NRR	11500000058-000	$ 75.00	$ 73.30
QTS	Enterprise Cloud - Additional Standard Firewall MRR	11511000130-000	$ 75.00	$ 73.30
QTS	Additional Site-To-Site VPN Connection MRR	11511000013-000	$ 80.00	$ 78.19

QTS	Managed VM Server (Includes HA VM OS Management & Licenses Monitoring 40GB useable storage RAID 5 SAN Storage) NRR	11500000005-000	$ 90.00	$ 87.96
QTS	Managed VPN MRR	10911100002-000	$ 91.97	$ 89.89
QTS	Dedicated Storage Management MRR	11011100066-000	$ 100.00	$ 97.73
QTS	Managed Network Hardware MRR	10911100021-000	$ 100.00	$ 97.73
QTS	Managed Network Hardware NRR	10900100021-000	$ 100.00	$ 97.73
QTS	Dedicated Storage Management NRR	11000100066-000	$ 100.00	$ 97.73
QTS	SQL Standard per 2 Core (Min 4 Core) MRR	11211100006-000	$ 119.99	$ 117.27
QTS	Remote Hands & Eyes - Pre-packaged MRR	10311100013-000	$ 120.00	$ 117.28
QTS	Remote Hands & Eyes - Pre-packaged NRR	10300100003-000	$ 120.00	$ 117.28
QTS	DR-HA VM with Replication MRR	11511000055-000	$ 120.00	$ 117.28
QTS	Remote Hands & Eyes MRR	10311100003-000	$ 125.00	$ 122.17
QTS	Remote Hands & Eyes NRR	10300100001-000	$ 125.00	$ 122.17
QTS	QVI - Windows Data Center MRR	11511000023-001	$ 125.00	$ 122.17
QTS	QVI - RedHat Advanced / Enterprise 2 Socket Physical MRR	11511000023-003	$ 125.00	$ 122.17
QTS	DR-VM with Replication MRR	11511000046-000	$ 135.00	$ 131.94
QTS	Virtual Load Balancing MRR	11511000009-000	$ 140.00	$ 136.83
QTS	Additional Subnet Setup Fee NRR	11500000007-000	$ 150.00	$ 146.60
QTS	Additional QVI IP addresses NRR	11500000012-000	$ 150.00	$ 146.60
QTS	QVI Additional SAN Storage NRR	11500000020-000	$ 150.00	$ 146.60
QTS	QVI Backup NRR	11500000039-000	$ 150.00	$ 146.60
QTS	DR-SAN Disk Capacity GBs NRR	11500000050-000	$ 150.00	$ 146.60
QTS	DRaaS - Physical Server replication (P2V) Set-up NRR	11500000142-000	$ 150.00	$ 146.60
QTS	Networking Services Custom MRR	10911100012-000	$ 169.48	$ 165.64
QTS	Networking Services Custom NRR	10900100016-000	$ 169.48	$ 165.64
QTS	Enterprise Cloud - Cloud Engineering Hourly Services MRR	11511000094-001	$ 175.00	$ 171.03
QTS	DRaaS - Physical Server replication (P2V) MRR	11511000142-000	$ 175.00	$ 171.03
QTS	QVI Base Support - Set-up NRR	11500000000-000	$ 200.00	$ 195.47
QTS	SERVER A -Small - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup)	11500000001-000	$ 200.00	$ 195.47
QTS	SERVER B - Medium Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup	11500000002-000	$ 200.00	$ 195.47
QTS	SERVER C -Large Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup) I	11500000003-000	$ 200.00	$ 195.47
QTS	SERVER D - Custom Config Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape	11500000004-000	$ 200.00	$ 195.47
QTS	Managed OS Windows MRR	10511100002-000	$ 202.41	$ 197.82
QTS	Managed OS Linux MRR	10511100004-000	$ 202.41	$ 197.82
QTS	Managed OS Solaris MRR	10511100006-000	$ 202.41	$ 197.82
QTS	Enterprise Cloud - Large Firewall MRR	11511000071-000	$ 225.00	$ 219.90
QTS	Enterprise Cloud - DR - Large Firewall MRR	11511000087-000	$ 225.00	$ 219.90
QTS	DRaaS - EC Reservation - Large Firewall MRR	11511000159-000	$ 225.00	$ 219.90
QTS	Basic Monitoring - Unmanaged MRR	10711100001-000	$ 46.06	$ 45.02
QTS	Basic Monitoring -Managed MRR	10711100002-000	$ 102.46	$ 100.14
QTS	Enhanced Monitoring - Unmanaged MRR	10711100003-000	$ 68.57	$ 67.02
QTS	Enhanced Monitoring - Managed MRR	10711100004-000	$ 124.97	$ 122.14
QTS	Advanced Monitoring - Unmanaged MRR	10711100005-000	$ 113.69	$ 111.11
QTS	Advanced Monitoring - Managed MRR	10711100006-000	$ 170.09	$ 166.23
QTS	Monitoring Internet Services - Unmanaged MRR	10711100013-000	$ 25.00	$ 24.43
QTS	Monitoring Internet Services - Managed MRR	10711100014-000	$ 100.00	$ 97.73
QTS	Monitoring Engineering T&M MRR	10711100021-000	$ 169.20	$ 165.36
QTS	Security Engineer T&M MRC NRR	10800100003-000	$ 170.00	$ 166.15
QTS	SOC Report - Second Report Distribution NRR	10800100005-000	$ 500.00	$ 488.66
QTS	DR - HA Physical Server Windows Data Center MRR	11511000058-000	$ 750.00	$ 733.00

QTS	SERVER B - Medium -Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backu	11511000002-000	$ 900.00	$ 879.60
QTS	DRaaS - Replication Service -Set-up NRR	11500000141-000	$ 1,000.00	$ 977.33
QTS	SERVER C - Large Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup) I	11511000003-000	$ 1,150.00	$ 1,123.93
QTS	SERVER D - Custom Config - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape	11511000004-000	$ 1,750.00	$ 1,710.33
QTS	DR - Additional Client to Site VPN MRR	11511000064-000	$ 8.00	$ 7.83
QTS	DR-VM Additional RAM GBs MRR	11511000048-000	$ 15.00	$ 14.66
QTS	DR-VM Additional VPU MRR	11511000049-000	$ 15.00	$ 14.66
QTS	DR- Additional Site to Site VPN MRR	11511000065-000	$ 25.00	$ 24.43
QTS	DR - HA Data Center Connect Base Fee MRR	11511000059-000	$ 200.00	$ 195.47
QTS	DR-On Demand Base Network MRR	11511000047-000	$ 340.00	$ 332.29
QTS	Federal Cloud - DR- Client to Site VPN (Qty 5) MRR	11500000123-000	$ 5.00	$ 4.89
QTS	Federal Cloud - Back-up services -GB Transferred MRR	11500000124-000	$ 0.24	$ 0.23
QTS	Federal Cloud - Cloud Engineering Services Hourly MRR	11511000094-000	$ 175.00	$ 171.03
QTS	VM Cloud Credit	11511000165-000	$ 1.00	$ 0.98
QTS	Advanced Monitoring - Managed NRR	10700100006-000	$ 67.68	$ 66.15
QTS	Monitoring Internet Services - Unmanaged NRR	10700100013-000	$ 50.00	$ 48.87
QTS	Monitoring Internet Services - Managed NRR	10700100014-000	$ 50.00	$ 48.87
QTS	Monitoring Engineering T&M NRR	10700100017-000	$ 169.20	$ 165.36
QTS	Managed Router MRR	10911100017-000	$ 239.12	$ 233.70
QTS	Managed OS Windows NRR	10500100002-000	$ 250.00	$ 244.33
QTS	Managed OS Linux NRR	10500100004-000	$ 250.00	$ 244.33
QTS	Managed OS Solaris NRR	10500100006-000	$ 250.00	$ 244.33
QTS	QVI Network Only - Connection back to Colo Space. (requires managed switch per standard cost). NRR	11500000015-000	$ 250.00	$ 244.33
QTS	Managed VM Server (Includes HA VM OS Management & Licenses Monitoring 40GB useable storage RAID 5 SAN Storage) MRR	11511000005-000	$ 250.00	$ 244.33
QTS	QVI Active Directory for Windows clustering MRR	11511000028-000	$ 250.00	$ 244.33
QTS	QVI - RedHat Advanced / Enterprise 4 Socket Physical MRR	11511000023-004	$ 250.00	$ 244.33
QTS	Managed Switch MRR	10911100009-000	$ 266.32	$ 260.28
QTS	Standard Load Balancing NRR	10900100006-000	$ 271.17	$ 265.02
QTS	QVI Base Support MRR	11511000000-000	$ 275.00	$ 268.77
QTS	Standard Load Balancing MRR	10911100006-000	$ 278.34	$ 272.03
QTS	DR - HA Physical Server Windows Standard-Linux MRR	11511000056-000	$ 280.00	$ 273.65
QTS	QVI Network - Pair of redundant virtual Firewalls 1 Site to Site VPN or 5 client to Site 1 Meg of Bandwidth MRR	11511000038-000	$ 285.00	$ 278.54
QTS	Managed OS AIX MRR	10511100007-000	$ 315.64	$ 308.48
QTS	HA Load Balancing MRR	10911100007-000	$ 326.51	$ 319.11
QTS	Managed VPN NRR	10900100002-000	$ 338.96	$ 331.28
QTS	On-Clouding MRR	11500000137-000	$ 350.00	$ 342.07
QTS	Firewall Management MRR	10911100004-000	$ 358.89	$ 350.75
QTS	DR-On Demand Base Network NRR	11500000047-000	$ 375.00	$ 366.50
QTS	Managed Switch NRR	10900100009-000	$ 406.78	$ 397.56
QTS	Firewall Management (HA Pair) MRR	10911100005-000	$ 407.06	$ 397.83
QTS	Managed OS AIX NRR	10500100007-000	$ 422.41	$ 412.83
QTS	HA Load Balancing NRR	10900100007-000	$ 440.65	$ 430.66
QTS	DR - HA Physical Server Windows Enterprise MRR	11511000057-000	$ 450.00	$ 439.80
QTS	SQL Enterprise - per 2 Core (Min 4 Core) MRR	11211100007-000	$ 460.15	$ 449.72
QTS	Managed Router NRR	10900100017-000	$ 474.55	$ 463.79
QTS	Firewall Management NRR	10900100004-000	$ 508.45	$ 496.92
QTS	QVI Network Only - Connection back to Colo Space. (requires managed switch per standard cost). MRR	11511000015-000	$ 600.00	$ 586.40
QTS	SERVER A - Small - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup)	11511000001-000	$ 675.00	$ 659.70
QTS	Firewall Management (HA Pair) NRR	10900100005-000	$ 677.93	$ 662.56

Salesforce.com	Console for Sales Cloud	204-1535	$ 120.00	$ 114.91
Salesforce.com	Console for Sales Cloud Government Cloud	204-1535GC	$ 36.00	$ 34.46
Salesforce.com	Identity Connect	204-1536	$ 12.00	$ 11.49
Salesforce.com	Identity Connect Government Cloud	204-1536GC	$ 3.60	$ 3.45
Salesforce.com	Pardot - Standard (price is per org)	204-1537	$ 12,000.00	$ 11,490.98
Salesforce.com	Pardot - Pro (price is per org)	204-1538	$ 24,000.00	$ 22,981.96
Salesforce.com	Pardot - Ultimate (price is per org)	204-1539	$ 36,000.00	$ 34,472.95
Salesforce.com	Premier Success Plan Professional Edition (Service Cloud)	204-1540	$ 117.00	$ 111.99
Salesforce.com	Premier Success Plan Enterprise Edition (Service Cloud)	204-1541	$ 243.00	$ 232.59
Salesforce.com	Premier+ Success Plan Professional Edition (Service Cloud)	204-1542	$ 195.00	$ 186.65
Salesforce.com	Premier+ Success Plan Enterprise Edition (Service Cloud)	204-1543	$ 405.00	$ 387.66
Salesforce.com	Premier Success Plan Enterprise Edition (Force Enterprise Edition)	204-1544	$ 144.00	$ 137.83
Salesforce.com	Premier+ Success Plan Enterprise Edition (Force Enterprise Edition)	204-1545	$ 240.00	$ 229.72
Salesforce.com	Customer Community Members Sandbox (100 Members)	204-1554	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Members Sandbox (500 Members)	204-1555	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members Sandbox (5000 Members)	204-1556	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Members Sandbox (25000 Members)	204-1557	$ 36,000.00	$ 34,458.44
Salesforce.com	Customer Community Members Sandbox (250000 Members)	204-1558	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Logins Sandbox (2000 Logins/Month)	204-1559	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Logins Sandbox (20000 Logins/Month)	204-1560	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Logins Sandbox (100000 Logins/Month)	204-1561	$ 36,000.00	$ 34,458.44
Salesforce.com	Customer Community Logins Sandbox (1000000 Logins/Month)	204-1562	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Plus (20 Members)	204-1563	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (20 Members) Government Cloud	204-1563GC	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members)	204-1564	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (100 Members) Government Cloud	204-1564GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month)	204-1565	$ 8,400.00	$ 8,040.30
Salesforce.com	Expansion Pack for PE	204-1148	$ 420.00	$ 402.19
Salesforce.com	Content Add-on for UE	204-1160	$ 420.00	$ 402.19
Salesforce.com	Content Edition for UE	204-1161	$ 420.00	$ 402.19
Salesforce.com	Ideas Only User	204-1163	$ 60.00	$ 57.45
Salesforce.com	Force.com Sites 1 Million Additional Page Views	204-1169	$ 12,000.00	$ 11,490.98
Salesforce.com	Marketing for PE	204-1170	$ 1,800.00	$ 1,723.65
Salesforce.com	Expansion Pack for PE Premium Support	204-1190	$ 63.00	$ 60.33
Salesforce.com	Web Services API for PE Premium Support	204-1191	$ 45.00	$ 43.09
Salesforce.com	Content Add-on for PE Premium Support	204-1192	$ 63.00	$ 60.33
Salesforce.com	Content Edition for PE Premium Support	204-1193	$ 63.00	$ 60.33
Salesforce.com	Salesforce for Force.com Edition Admin for EE Premium Support	204-1194	$ 90.00	$ 86.19
Salesforce.com	Salesforce Mobile for Partner Portal for EE Premium Support	204-1195	$ 45.00	$ 43.09
Salesforce.com	Sales Cloud Group Edition	204-1300	$ 300.00	$ 287.27
Salesforce.com	Sales Cloud Professional Edition	204-1301	$ 780.00	$ 746.91
Salesforce.com	Sales Cloud Enterprise Edition	204-1302	$ 1,500.00	$ 1,436.37
Salesforce.com	Sales Cloud Enterprise Edition Government Cloud	204-1302GC	$ 450.00	$ 430.73
Salesforce.com	Sales Cloud Unlimited Edition	204-1303	$ 3,000.00	$ 2,872.75
Salesforce.com	Sales Cloud Unlimited Edition Government Cloud	204-1303GC	$ 150.00	$ 143.58
Salesforce.com	Sales Cloud Contact Manager Edition	204-1304	$ 60.00	$ 57.45
Salesforce.com	Service Cloud Professional Edition	204-1305	$ 780.00	$ 746.91
Salesforce.com	Service Cloud Enterprise Edition	204-1306	$ 1,620.00	$ 1,551.28
Salesforce.com	Service Cloud Enterprise Edition Government Cloud	204-1306GC	$ 486.00	$ 465.19

Salesforce.com	Service Cloud Unlimited Edition	204-1307	$ 3,120.00	$ 2,987.66
Salesforce.com	Service Cloud Unlimited Edition Government Cloud	204-1307GC	$ 156.00	$ 149.32
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition	204-1308	$ 2,220.00	$ 2,125.83
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Government Cloud	204-1308GC	$ 666.00	$ 637.48
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition	204-1309	$ 3,720.00	$ 3,562.21
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Government Cloud	204-1309GC	$ 186.00	$ 178.04
Salesforce.com	Chatter Plus Professional	204-1310	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Enterprise	204-1311	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Enterprise Government Cloud	204-1311GC	$ 54.00	$ 51.69
Salesforce.com	Chatter Plus Unlimted	204-1312	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Unlimted Government Cloud	204-1312GC	$ 9.00	$ 8.61
Salesforce.com	Knowledge Only Enterprise Edition	204-1313	$ 600.00	$ 574.55
Salesforce.com	Knowledge Only Enterprise Edition Government Cloud	204-1313GC	$ 180.00	$ 172.29
Salesforce.com	Knowledge Only Unlimited Edition	204-1314	$ 600.00	$ 574.55
Salesforce.com	Knowledge Only Unlimited Edition Government Cloud	204-1314GC	$ 30.00	$ 28.72
Salesforce.com	Force.com Enterprise Edition	204-1315	$ 600.00	$ 574.55
Salesforce.com	Force.com Enterprise Edition Government Cloud	204-1315GC	$ 288.00	$ 275.67
Salesforce.com	Force.com Unlimited Edition	204-1316	$ 900.00	$ 861.82
Salesforce.com	Force.com Unlimited Edition Government Cloud	204-1316GC	$ 90.00	$ 86.15
Salesforce.com	Force.com (One App) Enterprise Edition	204-1317	$ 180.00	$ 172.36
Salesforce.com	Force.com (One App) Unlimted Edition	204-1318	$ 180.00	$ 172.36
Salesforce.com	Force.com (Admin) Enterprise Edition	204-1319	$ 600.00	$ 574.55
Salesforce.com	Force.com (Admin) Unlimited Edition	204-1320	$ 900.00	$ 861.82
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Professional	204-1321	$ 300.00	$ 287.27
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Enterprise	204-1322	$ 300.00	$ 287.27
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Unlimted	204-1323	$ 300.00	$ 287.27
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org) Enterprise	204-1324	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org) Unlimited	204-1325	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics - 1 Add'l Sched. Dashboards per Hour (price is per org) Enterprise	204-1326	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Dashboards per Hour (price is per org) Unlimited	204-1327	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Reports per Hour (price is per org) Enterprise	204-1328	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Reports per Hour (price is per org) Unlimted	204-1329	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Snapshots per Hour (price is per org) Enterprise	204-1330	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Snapshots per Hour (price is per org) Unlimited	204-1331	$ 6,000.00	$ 5,745.49
Salesforce.com	Data Storage (50MB) (price is per org) Group Edition	204-1332	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Professional Edition	204-1333	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Enterprise Edition	204-1334	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Enterprise Edition Government Cloud	204-1334GC	$ 90.00	$ 86.15
Salesforce.com	Data Storage (50MB) (price is per org) Unlimited Edition	204-1335	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Unlimited Edition Government Cloud	204-1335GC	$ 15.00	$ 14.36
Salesforce.com	Data Storage (500MB) (price is per org) Group Edition	204-1336	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Professional Edition	204-1337	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Enterprise Edition	204-1338	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Enterprise Edition Government Cloud	204-1338GC	$ 450.00	$ 430.73
Salesforce.com	Data Storage (500MB) (price is per org) Unlimited Edition	204-1339	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Unlimited Edition Government Cloud	204-1339GC	$ 75.00	$ 71.79
Salesforce.com	Expansion Pack Professional Edition	204-1340	$ 420.00	$ 402.19
Salesforce.com	Expansion Pack Enterprise Edition	204-1341	$ 420.00	$ 402.19
Salesforce.com	File Storage (1GB) (price is per org)	204-1342	$ 60.00	$ 57.45

Salesforce.com	File Storage (1GB) (price is per org) Government Cloud	204-1342GC	$ 18.00	$ 17.23
Salesforce.com	File Storage (10GB) (price is per org)	204-1343	$ 498.00	$ 476.88
Salesforce.com	File Storage (10GB) (price is per org) Government Cloud	204-1343GC	$ 149.40	$ 143.00
Salesforce.com	Heroku Starter	204-1344	$ 48,000.00	$ 45,963.93
Salesforce.com	Heroku Small	204-1345	$ 96,000.00	$ 91,927.86
Salesforce.com	Heroku Medium	204-1346	$ 192,000.00	$ 183,855.72
Salesforce.com	Heroku Large	204-1347	$ 384,000.00	$ 367,711.44
Salesforce.com	Knowledge Enterprise Edition	204-1348	$ 600.00	$ 574.55
Salesforce.com	Knowledge Unlimted Edition	204-1349	$ 600.00	$ 574.55
Salesforce.com	Live Agent Enterprise Edition	204-1350	$ 600.00	$ 574.55
Salesforce.com	Live Agent Unlimted Edition	204-1351	$ 600.00	$ 574.55
Salesforce.com	Mobile	204-1352	$ 600.00	$ 574.55
Salesforce.com	Offline	204-1353	$ 300.00	$ 287.27
Salesforce.com	Profiles and Page Layouts	204-1354	$ 300.00	$ 287.27
Salesforce.com	Salesforce for Google Apps	204-1355	$ 120.00	$ 114.91
Salesforce.com	Web Services API	204-1362	$ 300.00	$ 287.27
Salesforce.com	Weekly Export Service (price per org)	204-1363	$ 600.00	$ 574.55
Salesforce.com	Site.com Contributor-only (User License)	204-1369	$ 240.00	$ 229.82
Salesforce.com	Site.com Publisher-only (User License)	204-1370	$ 1,500.00	$ 1,436.37
Salesforce.com	Site.com Contributor (Feature License)	204-1371	$ 240.00	$ 229.82
Salesforce.com	Site.com Publisher (Feature License)	204-1372	$ 1,500.00	$ 1,436.37
Salesforce.com	Site.com Published Site (price is per site)	204-1373	$ 18,000.00	$ 17,236.47
Salesforce.com	Database.com (Standard Users)	204-1374	$ 120.00	$ 114.91
Salesforce.com	Database.com (100 Lite Users)	204-1375	$ 120.00	$ 114.91
Salesforce.com	Database.com (Administrator)	204-1376	$ 120.00	$ 114.91
Salesforce.com	Additional Records (100000) (price is per org)	204-1377	$ 120.00	$ 114.91
Salesforce.com	Additional Transactions (5000 per day) (price is per org)	204-1378	$ 120.00	$ 114.91
Salesforce.com	Authenticated Sites (100 Named Users)	204-1379	$ 1,200.00	$ 1,149.10
Salesforce.com	Authenticated Sites (1000 Named Users)	204-1380	$ 6,000.00	$ 5,745.49
Salesforce.com	Authenticated Sites (5000 Named Users)	204-1381	$ 18,000.00	$ 17,236.47
Salesforce.com	Authenticated Sites (25000 Named Users)	204-1382	$ 60,000.00	$ 57,454.91
Salesforce.com	Authenticated Sites (5000 Logins/month)	204-1383	$ 6,000.00	$ 5,745.49
Salesforce.com	Authenticated Sites (20000 Logins/month)	204-1384	$ 18,000.00	$ 17,236.47
Salesforce.com	Authenticated Sites (100000 Logins/month)	204-1385	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (100 Named Users)	204-1386	$ 6,000.00	$ 5,745.49
Salesforce.com	Service Cloud Portal (1000 Named Users)	204-1387	$ 24,000.00	$ 22,981.96
Salesforce.com	Service Cloud Portal (5000 Named Users)	204-1388	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (25000 Named Users)	204-1389	$ 120,000.00	$ 114,909.82
Salesforce.com	Service Cloud Portal (5000 Logins/month)	204-1390	$ 24,000.00	$ 22,981.96
Salesforce.com	Service Cloud Portal (20000 Logins/month)	204-1391	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (100000 Logins/month)	204-1392	$ 120,000.00	$ 114,909.82
Salesforce.com	Customer Portal - Enterprise Administration (1 Login/mo)	204-1393	$ 48.00	$ 45.96
Salesforce.com	Customer Portal - Enterprise Administration (Named User)	204-1394	$ 120.00	$ 114.91
Salesforce.com	Partner Portal (Named User)	204-1395	$ 420.00	$ 402.19
Salesforce.com	Content for Partner Portal and Customer Portal	204-1396	$ 420.00	$ 402.19
Salesforce.com	Mobile for Partner Portal	204-1397	$ 300.00	$ 287.27
Salesforce.com	Sites Pageviews (1 Million/month) - (price is per org)	204-1398	$ 12,000.00	$ 11,490.98
Salesforce.com	Chatter Answers for Portal Users (Logins/month)	204-1399	$ 2.40	$ 2.30
Salesforce.com	Chatter Answers for Portal Users (Named)	204-1400	$ 12.00	$ 11.49

Salesforce.com	Marketing Cloud Package Enterprise	204-1401	$ 480,000.00	$ 459,639.29
Salesforce.com	Radian6 Basic	204-1402	$ 12,000.00	$ 11,490.98
Salesforce.com	Radian6 Pro	204-1403	$ 36,000.00	$ 34,472.95
Salesforce.com	Radian6 Corporate	204-1404	$ 96,000.00	$ 91,927.86
Salesforce.com	Radian6 Enterprise	204-1405	$ 348,000.00	$ 333,238.49
Salesforce.com	R6 Add on Insights Credits (10000)	204-1406	$ 1,200.00	$ 1,149.10
Salesforce.com	R6 Add on 50000 additional mentions	204-1407	$ 12,000.00	$ 11,490.98
Salesforce.com	R6 Add on 1 million additional mentions	204-1408	$ 60,000.00	$ 57,454.91
Salesforce.com	R6 Add on Social Accounts	204-1409	$ 9,000.00	$ 8,618.24
Salesforce.com	R6 Add on PT: Optimize Your Topic Profile	204-1410	$ 3,000.00	$ 2,872.75
Salesforce.com	R6 Add on Topic Management Service (1 x fee)	204-1411	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Topic management Service (monthly)	204-1412	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Topic Management Service (TSS)	204-1413	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Rapid TSS (RTSS)	204-1414	$ 12,000.00	$ 11,490.98
Salesforce.com	R6 Add on TSS/RTSS Additional Keyword	204-1415	$ 1,800.00	$ 1,723.65
Salesforce.com	R6 Add on TSS/RTSS Additional Dashboard	204-1416	$ 3,000.00	$ 2,872.75
Salesforce.com	Brand Overview Report	204-1417	$ 5,000.00	$ 4,787.91
Salesforce.com	On-Site Training (Price is per day + expenses minimum 2 days)	204-1418	$ 2,500.00	$ 2,393.95
Salesforce.com	Social Media Analyst (on going) FT	204-1419	$ 108,000.00	$ 103,418.84
Salesforce.com	Social Media Analyst (on going) HT	204-1420	$ 60,000.00	$ 57,454.91
Salesforce.com	Social Media Senior Analyst (on-going) FT	204-1421	$ 144,000.00	$ 137,891.79
Salesforce.com	Social Media Senior Analyst (on-going) HT	204-1422	$ 78,000.00	$ 74,691.39
Salesforce.com	Project Manager FT	204-1423	$ 192,000.00	$ 183,855.72
Salesforce.com	Project Manager HT	204-1424	$ 103,680.00	$ 99,282.09
Salesforce.com	Project Manager QT	204-1425	$ 59,520.00	$ 56,995.27
Salesforce.com	Command Center CVE (on-going)	204-1426	$ 5,000.00	$ 4,787.91
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (1-499 users)	204-1427	$ 125.00	$ 119.70
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (500-2000 users)	204-1428	$ 89.00	$ 85.22
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (2000+ users)	204-1429	$ 70.00	$ 67.03
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (1-499 users)	204-1430	$ 154.00	$ 147.47
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (500-2000 users)	204-1431	$ 111.00	$ 106.29
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (2000+ users)	204-1432	$ 85.00	$ 81.39
Salesforce.com	ISV Portal Bundle for Acumen Schoolforce Gold Application (Bundles include 100 ISV Portal licenses)	204-1433	$ 341.00	$ 326.54
Salesforce.com	Data Storage for Schoolforce Gold (500MB) (price is per org)	204-1434	$ 2,273.00	$ 2,176.58
Salesforce.com	Marketing Cloud Package Basic	204-1435	$ 60,000.00	$ 57,454.91
Salesforce.com	Marketing Cloud Package Pro	204-1436	$ 120,000.00	$ 114,909.82
Salesforce.com	Marketing Cloud Package Corporate	204-1437	$ 240,000.00	$ 229,819.65
Salesforce.com	Buddy Media Enterprise	204-1438	$ 480,000.00	$ 459,639.29
Salesforce.com	Buddy Media (stand alone)	204-1439	$ 45,000.00	$ 43,091.18
Salesforce.com	Buddy Social Accounts	204-1440	$ 9,000.00	$ 8,618.24
Salesforce.com	Buddy Media 1 million additional open web sharing PV's	204-1441	$ 1,020.00	$ 976.73
Salesforce.com	Buddy Media 1 million additional open web syndication PV's	204-1442	$ 1,020.00	$ 976.73
Salesforce.com	Buy Buddy	204-1443	$ 6,000.00	$ 5,745.49
Salesforce.com	Buddy Social Account Reports	204-1444	$ 9,600.00	$ 9,192.79
Salesforce.com	Buddy Aggregate Dashboard Reports	204-1445	$ 12,000.00	$ 11,490.98
Salesforce.com	Buddy Quarterly Content	204-1446	$ 44,400.00	$ 42,516.63
Salesforce.com	Buddy One-time content	204-1447	$ 132,000.00	$ 126,400.81
Salesforce.com	Buddy Quarterly Competitive Intelligence Analysis	204-1448	$ 84,000.00	$ 80,436.88
Salesforce.com	Buddy One-time Competitive Intelligence Analysis	204-1449	$ 24,000.00	$ 22,981.96

Salesforce.com	Buddy Quarterly Facebook Wall or Twitter Optimization Analysis	204-1450	$ 16,800.00	$ 16,087.38
Salesforce.com	Buddy One time Facebook Wall or Twitter Optimization Analysis	204-1451	$ 48,000.00	$ 45,963.93
Salesforce.com	Force.com (1 Enterprise Application) Enterprise Edition	204-1452	$ 300.00	$ 287.15
Salesforce.com	Force.com (1 Enterprise Application) Enterprise Edition Government Cloud	204-1452GC	$ 90.00	$ 86.15
Salesforce.com	Force.com (1 Enterprise Application) Unlimited Edition	204-1453	$ 300.00	$ 287.15
Salesforce.com	Force.com (1 Enterprise Application) Unlimited Edition Government Cloud	204-1453GC	$ 15.00	$ 14.36
Salesforce.com	Force.com (1 Light Application) Enterprise Edition	204-1454	$ 120.00	$ 114.86
Salesforce.com	Force.com (1 Light Application) Enterprise Edition Government Cloud	204-1454GC	$ 36.00	$ 34.46
Salesforce.com	Force.com (1 Light Application) Unlimited Edition	204-1455	$ 120.00	$ 114.86
Salesforce.com	Force.com (1 Light Application) Unlimited Edition Government Cloud	204-1455GC	$ 6.00	$ 5.74
Salesforce.com	Force.com (Administrator) User Subscription Enterprise Edition	204-1456	$ 600.00	$ 574.31
Salesforce.com	Force.com (Administrator) User Subscription Enterprise Edition Government Cloud	204-1456GC	$ 180.00	$ 172.29
Salesforce.com	Force.com (Administrator) User Subscription Unlimited Edition	204-1457	$ 900.00	$ 861.46
Salesforce.com	Force.com (Administrator) User Subscription Unlimited Edition Government Cloud	204-1457GC	$ 45.00	$ 43.07
Salesforce.com	Remedyforce (BMC)	204-1458	$ 948.00	$ 907.41
Salesforce.com	Data Storage (50MB) (price is per org)	204-1459	$ 300.00	$ 287.27
Salesforce.com	Data Storage (500MB) (price is per org)	204-1460	$ 1,500.00	$ 1,436.37
Salesforce.com	Data.com Corporate Clean	204-1461	$ 300.00	$ 287.27
Salesforce.com	Data.com Corporate Prospector	204-1462	$ 1,500.00	$ 1,436.37
Salesforce.com	Data.com Corporate Records Additional (price is each)	204-1463	$ 0.50	$ 0.48
Salesforce.com	Data.com Premium Clean	204-1464	$ 420.00	$ 402.18
Salesforce.com	Data.com Premium Prospector	204-1465	$ 1,980.00	$ 1,896.01
Salesforce.com	Data.com Premium Records Additional (price is each)	204-1466	$ 0.65	$ 0.62
Salesforce.com	Data.com Services - QuickStart	204-1467	$ 5,000.00	$ 4,787.91
Salesforce.com	Partner Community Members (20 Members)	204-1468	$ 8,400.00	$ 8,043.69
Salesforce.com	Partner Community Members (20 Members) Government Cloud	204-1468GC	$ 2,520.00	$ 2,412.09
Salesforce.com	Partner Community Members (100 Members)	204-1469	$ 30,000.00	$ 28,727.46
Salesforce.com	Partner Community Members (100 Members) Government Cloud	204-1469GC	$ 9,000.00	$ 8,614.61
Salesforce.com	Partner Community Members (500 Members)	204-1470	$ 96,000.00	$ 91,927.86
Salesforce.com	Partner Community Members (500 Members) Government Cloud	204-1470GC	$ 28,800.00	$ 27,566.75
Salesforce.com	Customer Community Members (500 Members)	204-1478	$ 12,000.00	$ 11,490.98
Salesforce.com	Customer Community Members (500 Members) Government Cloud	204-1478GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members (250000 Members)	204-1481	$ 600,000.00	$ 574,549.12
Salesforce.com	Customer Community Members (250000 Members) Government Cloud	204-1481GC	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Logins (2000 Logins/Month)	204-1482	$ 12,000.00	$ 11,490.98
Salesforce.com	Customer Community Logins (2000 Logins/Month) Government Cloud	204-1482GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Logins (100000 Logins/Month)	204-1484	$ 120,000.00	$ 114,909.82
Salesforce.com	Customer Community Logins (1000000 Logins/Month)	204-1485	$ 600,000.00	$ 574,549.12
Salesforce.com	Customer Community Logins (1000000 Logins/Month) Government Cloud	204-1485GC	$ 180,000.00	$ 172,292.19
Salesforce.com	Sales Cloud Performance Edition	204-1486	$ 3,420.00	$ 3,274.93
Salesforce.com	Service Cloud Performance Edition	204-1487	$ 3,420.00	$ 3,274.93
Salesforce.com	Service Cloud Knowledge Pack Performance Edition	204-1488	$ 3,420.00	$ 3,274.93
Salesforce.com	Company Community Only	204-1489	$ 240.00	$ 229.82
Salesforce.com	Identity Only	204-1490	$ 60.00	$ 57.45
Salesforce.com	Identity Only Government Cloud	204-1490GC	$ 18.00	$ 17.23
Salesforce.com	Work.com Motivate	204-1491	$ 120.00	$ 114.91
Salesforce.com	Work.com Align	204-1492	$ 180.00	$ 172.36
Salesforce.com	Work.com Perform	204-1493	$ 240.00	$ 229.82
Salesforce.com	Force.com Performance	204-1494	$ 1,800.00	$ 1,723.65

Salesforce.com	Force.com Performance (Admin)	204-1495	$ 900.00	$ 861.82
Salesforce.com	Partner Community Members Sandbox (20 Members)	204-1498	$ 2,520.00	$ 2,413.11
Salesforce.com	Partner Community Members Sandbox (100 Members)	204-1499	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Members Sandbox (500 Members)	204-1500	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Members Sandbox (2500 Members)	204-1501	$ 126,000.00	$ 120,655.31
Salesforce.com	Partner Community Members Sandbox (10000 Members)	204-1502	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Logins Sandbox (200 Logins/Month)	204-1503	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Logins Sandbox (1000 Logins/Month)	204-1504	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Logins Sandbox (5000 Logins/Month)	204-1505	$ 126,000.00	$ 120,655.31
Salesforce.com	Partner Community Logins Sandbox (20000 Logins/Month)	204-1506	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Members Premier Support (20 Members)	204-1507	$ 1,260.00	$ 1,206.55
Salesforce.com	Partner Community Members Premier Support (100 Members)	204-1508	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Members Premier Support (500 Members)	204-1509	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Members Premier Support (2500 Members)	204-1510	$ 63,000.00	$ 60,327.66
Salesforce.com	Partner Community Members Premier Support (10000 Members)	204-1511	$ 225,000.00	$ 215,455.92
Salesforce.com	Partner Community Logins Premier Support (200 Logins/Month)	204-1512	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Logins Premier Support (1000 Logins/Month)	204-1513	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Logins Premier Support (5000 Logins/Month)	204-1514	$ 63,000.00	$ 60,327.66
Salesforce.com	Partner Community Logins Premier Support (20000 Logins/Month)	204-1515	$ 225,000.00	$ 215,455.92
Salesforce.com	Partner Community Members Premier Support+ (20 Members)	204-1516	$ 2,100.00	$ 2,010.92
Salesforce.com	Partner Community Members Premier Support+ (100 Members)	204-1517	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Members Premier Support+ (500 Members)	204-1518	$ 24,000.00	$ 22,981.96
Salesforce.com	Partner Community Members Premier Support+ (2500 Members)	204-1519	$ 105,000.00	$ 100,546.10
Salesforce.com	Partner Community Members Premier Support+ (10000 Members)	204-1520	$ 375,000.00	$ 359,093.20
Salesforce.com	Partner Community Logins Premier Support+ (200 Logins/Month)	204-1521	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Logins Premier Support+ (1000 Logins/Month)	204-1522	$ 24,000.00	$ 22,981.96
Salesforce.com	Partner Community Logins Premier Support+ (5000 Logins/Month)	204-1523	$ 105,000.00	$ 100,546.10
Salesforce.com	Partner Community Logins Premier Support+ (20000 Logins/Month)	204-1525	$ 375,000.00	$ 359,093.20
Salesforce.com	Force.com EE	204-1526	$ 960.00	$ 919.28
Salesforce.com	Force.com UE	204-1527	$ 1,800.00	$ 1,723.65
Salesforce.com	Force.com PXE	204-1528	$ 1,800.00	$ 1,723.65
Salesforce.com	Sales Cloud Group Edition Premier + Success Plan	204-1300PPS	$ 75.00	$ 71.82
Salesforce.com	Sales Cloud Group Edition Premier Success Plan	204-1300PS	$ 45.00	$ 43.09
Salesforce.com	Sales Cloud Group Edition Sandbox (Developer Pro)	204-1300SBD	$ 15.00	$ 14.36
Salesforce.com	Sales Cloud Group Edition Sandbox (Full Copy)	204-1300SBF	$ 90.00	$ 86.18
Salesforce.com	Sales Cloud Group Edition Sandbox (Partial Copy)	204-1300SBP	$ 60.00	$ 57.45
Salesforce.com	Sales Cloud Professional Edition Premier + Success	204-1301PPS	$ 195.00	$ 186.73
Salesforce.com	Sales Cloud Professional Edition Premier Success	204-1301PS	$ 117.00	$ 112.04
Salesforce.com	Sales Cloud Professional Edition Sandbox (Developer Pro)	204-1301SBD	$ 39.00	$ 37.35
Salesforce.com	Sales Cloud Professional Edition Sandbox (Full Copy)	204-1301SBF	$ 234.00	$ 224.07
Salesforce.com	Sales Cloud Professional Edition Sandbox (Partial Copy)	204-1301SBP	$ 156.00	$ 149.38
Salesforce.com	Sales Cloud Enterprise Edition Premier + Success	204-1302PPS	$ 375.00	$ 359.09
Salesforce.com	Sales Cloud Enterprise Edition Premier Success	204-1302PS	$ 225.00	$ 215.46
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Developer Pro)	204-1302SBD	$ 75.00	$ 71.82
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Full Copy)	204-1302SBF	$ 450.00	$ 430.91
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Partial Copy)	204-1302SBP	$ 300.00	$ 287.27
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Developer Pro)	204-1303SBD	$ 150.00	$ 143.64
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Full Copy)	204-1303SBF	$ 900.00	$ 861.82
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Partial Copy)	204-1303SBP	$ 600.00	$ 574.55

Salesforce.com	Sales Cloud Contact Manager Edition Government Cloud	204-1304GC	$ 18.00	$ 17.24
Salesforce.com	Sales Cloud Contact Manager Edition Premier + Success	204-1304PPS	$ 15.00	$ 14.36
Salesforce.com	Sales Cloud Contact Manager Edition Premier Success	204-1304PS	$ 9.00	$ 8.62
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Developer Pro)	204-1304SBD	$ 3.00	$ 2.87
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Full Copy)	204-1304SBF	$ 18.00	$ 17.24
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Partial Copy)	204-1304SBP	$ 12.00	$ 11.49
Salesforce.com	Service Cloud Professional Edition Government Cloud	204-1305GC	$ 234.00	$ 224.07
Salesforce.com	Service Cloud Professional Edition Premier + Success	204-1305PPS	$ 195.00	$ 186.73
Salesforce.com	Service Cloud Professional Edition Premier Success	204-1305PS	$ 117.00	$ 112.04
Salesforce.com	Service Cloud Professional Edition Sandbox (Developer Pro)	204-1305SBD	$ 39.00	$ 37.35
Salesforce.com	Service Cloud Professional Edition Sandbox (Full Copy)	204-1305SBF	$ 234.00	$ 224.07
Salesforce.com	Service Cloud Professional Edition Sandbox (Partial Copy)	204-1305SBP	$ 156.00	$ 149.38
Salesforce.com	Service Cloud Enterprise Edition Premier + Success	204-1306PPS	$ 405.00	$ 387.82
Salesforce.com	Service Cloud Enterprise Edition Premier Success	204-1306PS	$ 243.00	$ 232.69
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Developer Pro)	204-1306SBD	$ 81.00	$ 77.56
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Full Copy)	204-1306SBF	$ 486.00	$ 465.38
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Partial Copy)	204-1306SBP	$ 324.00	$ 310.26
Salesforce.com	Service Cloud Unlimted Edition Sandbox (Developer Pro)	204-1307SBD	$ 156.00	$ 149.38
Salesforce.com	Service Cloud Unlimited Edition Sandbox (Full Copy)	204-1307SBF	$ 936.00	$ 896.30
Salesforce.com	Service Cloud Unlimted Edition Sandbox (Partial Copy)	204-1307SBP	$ 624.00	$ 597.53
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Developer Pro)	204-1308SBD	$ 111.00	$ 106.29
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Full Copy)	204-1308SBF	$ 666.00	$ 637.75
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Partial Copy)	204-1308SBP	$ 444.00	$ 425.17
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Developer Pro)	204-1309SBD	$ 186.00	$ 178.11
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Full Copy)	204-1309SBF	$ 1,116.00	$ 1,068.66
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Partial Copy)	204-1309SBP	$ 744.00	$ 712.44
Salesforce.com	Force.com Enterprise Edition Premier + Success	204-1315PPS	$ 930.00	$ 890.55
Salesforce.com	Force.com Enterprise Edition Premier Success	204-1315PS	$ 558.00	$ 534.33
Salesforce.com	Force.com Enterprise Edition Sandbox (Developer Pro)	204-1315SBD	$ 186.00	$ 178.11
Salesforce.com	Force.com Enterprise Edition Sandbox (Full Copy)	204-1315SBF	$ 1,116.00	$ 1,068.66
Salesforce.com	Force.com Enterprise Edition Sandbox (Partial Copy)	204-1315SBP	$ 744.00	$ 712.44
Salesforce.com	Force.com (Admin) Enterprise Edition Government Cloud	204-1319GC	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Enterprise Edition Premier + Success	204-1319PPS	$ 225.00	$ 215.46
Salesforce.com	Force.com (Admin) Enterprise Edition Premier Success	204-1319PS	$ 135.00	$ 129.27
Salesforce.com	Force.com (Admin) Enterprise Edition Sandbox (Developer Pro)	204-1319SBD	$ 45.00	$ 43.09
Salesforce.com	Force.com (Admin) Enterprise Edition Sandbox (Full Copy)	204-1319SBF	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Government Cloud	204-1320GC	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Developer Pro)	204-1320SBD	$ 45.00	$ 43.09
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Full Copy)	204-1320SBF	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Partial Copy)	204-1320SBP	$ 180.00	$ 172.36
Salesforce.com	Sales Cloud Performance Edition Sandbox (Developer Pro)	204-1486SBD	$ 171.00	$ 163.75
Salesforce.com	Sales Cloud Performance Edition Sandbox (Full Copy)	204-1486SBF	$ 1,026.00	$ 982.48
Salesforce.com	Sales Cloud Performance Edition Sandbox (Partial Copy)	204-1486SBP	$ 684.00	$ 654.99
Salesforce.com	Service Cloud Performance Edition Sandbox (Developer Pro)	204-1487SBD	$ 171.00	$ 163.75
Salesforce.com	Service Cloud Performance Edition Sandbox (Full Copy)	204-1487SBF	$ 1,026.00	$ 982.48
Salesforce.com	Service Cloud Performance Edition Sandbox (Partial Copy)	204-1487SBP	$ 684.00	$ 654.99
Salesforce.com	Force.com EE Government Cloud	204-1526GC	$ 288.00	$ 275.78
Salesforce.com	Force.com EE Premier + Success	204-1526PPS	$ 240.00	$ 229.82
Salesforce.com	Force.com EE Premier Success	204-1526PS	$ 144.00	$ 137.89

Salesforce.com	Force.com EE Sandbox (Developer Pro)	204-1526SBD	$ 48.00	$ 45.96
Salesforce.com	Force.com EE Sandbox (Full Copy)	204-1526SBF	$ 288.00	$ 275.78
Salesforce.com	Force.com EE Sandbox (Partial Copy)	204-1526SBP	$ 192.00	$ 183.86
Salesforce.com	Force.com UE Government Cloud	204-1527GC	$ 540.00	$ 517.09
Salesforce.com	Force.com UE Sandbox (Developer Pro)	204-1527SBD	$ 90.00	$ 86.18
Salesforce.com	Force.com UE Sandbox (Full Copy)	204-1527SBF	$ 540.00	$ 517.09
Salesforce.com	Force.com UE Sandbox (Partial Copy)	204-1527SBP	$ 360.00	$ 344.73
Salesforce.com	Force.com PXE Sandbox (Developer Pro)	204-1528SBD	$ 90.00	$ 86.18
Salesforce.com	Force.com PXE Sandbox (Full Copy)	204-1528SBF	$ 540.00	$ 517.09
Salesforce.com	Force.com PXE Sandbox (Partial Copy)	204-1528SBP	$ 360.00	$ 344.73
Salesforce.com	Additional Scheduled Analytics Bundle (price is per org)	204-1582	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org)	204-1583	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics Cloud - Wave Platform	204-1584	$ 480,000.00	$ 459,639.29
Salesforce.com	Analytics Cloud - Builder	204-1585	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics Cloud - Explorer	204-1586	$ 1,500.00	$ 1,436.37
Salesforce.com	Console for Sales Cloud	204-1587	$ 120.00	$ 114.91
Salesforce.com	Data Storage (10GB) (price is per org)	204-1588	$ 12,000.00	$ 11,490.98
Salesforce.com	File Storage (1TB) (price is per org)	204-1589	$ 3,600.00	$ 3,447.29
Salesforce.com	Customer Community Members (5000 Members)	204-1479	$ 52,800.00	$ 50,539.04
Salesforce.com	Customer Community Members (5000 Members) Government Cloud	204-1479GC	$ 15,840.00	$ 15,161.71
Salesforce.com	Customer Community Members (25000 Members)	204-1480	$ 132,000.00	$ 126,347.61
Salesforce.com	Customer Community Members (25000 Members) Government Cloud	204-1480GC	$ 39,600.00	$ 37,904.28
Salesforce.com	Customer Community Logins (20000 Logins/Month)	204-1483	$ 52,800.00	$ 50,539.04
Salesforce.com	Customer Community Logins (20000 Logins/Month) Government Cloud	204-1483GC	$ 15,840.00	$ 15,161.71
Salesforce.com	Partner Community Members (2500 Members)	204-1471	$ 384,000.00	$ 367,556.68
Salesforce.com	Partner Community Members (2500 Members) Government Cloud	204-1471GC	$ 115,200.00	$ 110,267.00
Salesforce.com	Partner Community Members Premier Support+ (2500 Members)	204-1471PPS	$ 96,000.00	$ 91,889.17
Salesforce.com	Partner Community Members Premier Support (2500 Members)	204-1471PS	$ 57,600.00	$ 55,133.50
Salesforce.com	Partner Community Members Sandbox (2500 Members)	204-1471SB	$ 115,200.00	$ 110,267.00
Salesforce.com	Partner Community Members (10000 Members)	204-1472	$ 810,000.00	$ 775,314.86
Salesforce.com	Partner Community Members (10000 Members) Government Cloud	204-1472GC	$ 243,000.00	$ 232,594.46
Salesforce.com	Partner Community Members Premier Support+ (10000 Members)	204-1472PPS	$ 202,500.00	$ 193,828.72
Salesforce.com	Partner Community Members Premier Support (10000 Members)	204-1472PS	$ 121,500.00	$ 116,297.23
Salesforce.com	Partner Community Logins (200 Logins/Month)	204-1473	$ 24,000.00	$ 22,972.29
Salesforce.com	Partner Community Logins (200 Logins/Month) Government Cloud	204-1473GC	$ 7,200.00	$ 6,891.69
Salesforce.com	Partner Community Logins Premier Support+ (200 Logins/Month)	204-1473PPS	$ 6,000.00	$ 5,743.07
Salesforce.com	Partner Community Logins Premier Support (200 Logins/Month)	204-1473PS	$ 3,600.00	$ 3,445.84
Salesforce.com	Partner Community Logins Sandbox (200 Logins/Month)	204-1473SB	$ 7,200.00	$ 6,891.69
Salesforce.com	Partner Community Logins (1000 Logins/Month)	204-1474	$ 78,000.00	$ 74,659.95
Salesforce.com	Partner Community Logins (1000 Logins/Month) Government Cloud	204-1474GC	$ 23,400.00	$ 22,397.98
Salesforce.com	Partner Community Logins Premier Support+ (1000 Logins/Month)	204-1474PPS	$ 19,500.00	$ 18,664.99
Salesforce.com	Partner Community Logins Premier Support (1000 Logins/Month)	204-1474PS	$ 11,700.00	$ 11,198.99
Salesforce.com	Partner Community Logins Sandbox (1000 Logins/Month)	204-1474SB	$ 23,400.00	$ 22,397.98
Salesforce.com	Partner Community Logins (5000 Logins/Month)	204-1475	$ 240,000.00	$ 229,722.92
Salesforce.com	Partner Community Logins (5000 Logins/Month) Government Cloud	204-1475GC	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins Premier Support+ (5000 Logins/Month)	204-1475PPS	$ 60,000.00	$ 57,430.73
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Sanbox (Developer Pro)	204-1641SBD	$ 8.00	$ 7.73
Salesforce.com	Salesforce Event Monitoring (10% of List Price per $100 of List Licence)	204-EM	$ 10.00	$ 9.65
Salesforce.com	Field Audit Trail (10% of List Price per $100 of List Licence)	204-FAT	$ 10.00	$ 9.65

Salesforce.com	Platform Encryption (20% of List Price per $100 of List Licence)	204-PLT-E	$ 20.00	$ 19.29
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Premier Success	204-1641PS	$ 24.00	$ 23.15
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Sanbox (Developer Pro)	204-1647SBD	$ 24.00	$ 23.15
Salesforce.com	Salesforce Shield (30% of List Price per $100 of List Licence)	204-SFS	$ 30.00	$ 28.94
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Sanbox (Developer Pro)	204-1644SBD	$ 30.00	$ 28.94
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members (Partial Copy)	204-1641SBP	$ 32.00	$ 30.87
Salesforce.com	Customer Community Members- 10 Members Sanbox (Developer Pro)	204-1631SBD	$ 40.00	$ 38.59
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Premier+ Success	204-1641PPS	$ 40.00	$ 38.59
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Government Cloud	204-1641GC	$ 48.00	$ 46.30
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Sandbox (Full Copy)	204-1641SBF	$ 48.00	$ 46.30
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Sanbox (Developer Pro)	204-1637SBD	$ 60.00	$ 57.88
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Premier Success	204-1647PS	$ 72.00	$ 69.45
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Premier Success	204-1644PS	$ 90.00	$ 86.82
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Sanbox (Developer Pro)	204-1645SBD	$ 96.00	$ 92.60
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members (Partial Copy)	204-1647SBP	$ 96.00	$ 92.60
Salesforce.com	Customer Community Plus- 10 Members Sanbox (Developer Pro)	204-1619SBD	$ 120.00	$ 115.76
Salesforce.com	Customer Community Members- 10 Members Premier Success	204-1631PS	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month (Partial Copy)	204-1644SBP	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Premier+ Success	204-1647PPS	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Government Cloud	204-1647GC	$ 144.00	$ 138.91
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Sandbox (Full Copy)	204-1647SBF	$ 144.00	$ 138.91
Salesforce.com	Customer Community Logins- 200 Logins/Month Sanbox (Developer Pro)	204-1634SBD	$ 150.00	$ 144.70
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Premier+ Success	204-1644PPS	$ 150.00	$ 144.70
Salesforce.com	Customer Community Members- 10 Members (Partial Copy)	204-1631SBP	$ 160.00	$ 154.34
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members	204-1641	$ 160.00	$ 154.34
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Premier Success	204-1637PS	$ 180.00	$ 173.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Government Cloud	204-1644GC	$ 180.00	$ 173.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Sandbox (Full Copy)	204-1644SBF	$ 180.00	$ 173.63
Salesforce.com	Customer Community Members- 10 Members Premier+ Success	204-1631PPS	$ 200.00	$ 192.93
Salesforce.com	Customer Community Member (100 Members) Sandbox (Developer Pro)	204-1477SBD	$ 210.00	$ 202.57
Salesforce.com	Customer Community Members- 10 Members Government Cloud	204-1631GC	$ 240.00	$ 231.51
Salesforce.com	Customer Community Members- 10 Members Sandbox (Full Copy)	204-1631SBF	$ 240.00	$ 231.51
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) (Partial Copy)	204-1637SBP	$ 240.00	$ 231.51
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Sanbox (Developer Pro)	204-1653SBD	$ 280.00	$ 270.10
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Premier Success	204-1645PS	$ 288.00	$ 277.81
Salesforce.com	Partner Community Members - 10 Members Sandbox (Developer Pro)	204-1612SBD	$ 300.00	$ 289.39
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Premier+ Success	204-1637PPS	$ 300.00	$ 289.39
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Sanbox (Developer Pro)	204-1646SBD	$ 300.00	$ 289.39
Salesforce.com	Customer Community Plus- 10 Members Premier Success	204-1619PS	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Government Cloud	204-1637GC	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Sandbox (Full Copy)	204-1637SBF	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Sanbox (Developer Pro)	204-1648SBD	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month (Partial Copy)	204-1645SBP	$ 384.00	$ 370.42
Salesforce.com	Customer Community Logins- 200 Logins/Month Premier Success	204-1634PS	$ 450.00	$ 434.09
Salesforce.com	Customer Community Logins- 1000 Logins/Month Sanbox (Developer Pro)	204-1635SBD	$ 450.00	$ 434.09
Salesforce.com	Customer Community Plus- 10 Members (Partial Copy)	204-1619SBP	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Sanbox (Developer Pro)	204-1642SBD	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Premier+ Success	204-1645PPS	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members	204-1647	$ 480.00	$ 463.02

Salesforce.com	Heroku - 1 Dyno	204-1610	$ 540.00	$ 520.90
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Government Cloud	204-1645GC	$ 576.00	$ 555.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Sandbox (Full Copy)	204-1645SBF	$ 576.00	$ 555.63
Salesforce.com	Data.com Premium Add on	204-1609	$ 600.00	$ 578.78
Salesforce.com	Customer Community Plus- 10 Members Premier+ Success	204-1619PPS	$ 600.00	$ 578.78
Salesforce.com	Customer Community Logins- 200 Logins/Month (Partial Copy)	204-1634SBP	$ 600.00	$ 578.78
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month	204-1644	$ 600.00	$ 578.78
Salesforce.com	Salesforce Engage	204-1673	$ 600.00	$ 578.78
Salesforce.com	Customer Community Member (500 Members) Sandbox (Developer Pro)	204-1478SBD	$ 600.00	$ 578.78
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Developer Pro)	204-1482SBD	$ 600.00	$ 578.78
Salesforce.com	Customer Community Member (100 Members) Premier Success	204-1477PS	$ 630.00	$ 607.72
Salesforce.com	Customer Community Plus- 10 Members Government Cloud	204-1619GC	$ 720.00	$ 694.54
Salesforce.com	Customer Community Plus- 10 Members Sandbox (Full Copy)	204-1619SBF	$ 720.00	$ 694.54
Salesforce.com	Customer Community Logins- 200 Logins/Month Premier+ Success	204-1634PPS	$ 750.00	$ 723.48
Salesforce.com	Customer Community Members- 10 Members	204-1631	$ 800.00	$ 771.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Premier Success	204-1653PS	$ 840.00	$ 810.29
Salesforce.com	Customer Community Member (100 Members) Sandbox (Partial Copy)	204-1477SBP	$ 840.00	$ 810.29
Salesforce.com	Partner Community Members - 10 Members Premier Success	204-1612PS	$ 900.00	$ 868.17
Salesforce.com	Customer Community Logins- 200 Logins/Month Government Cloud	204-1634GC	$ 900.00	$ 868.17
Salesforce.com	Customer Community Logins- 200 Logins/Month Sandbox (Full Copy)	204-1634SBF	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Premier Success	204-1646PS	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Sanbox (Developer Pro)	204-1654SBD	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Developer Pro)	204-1640SBD	$ 960.00	$ 926.05
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Sanbox (Developer Pro)	204-1643SBD	$ 1,020.00	$ 983.93
Salesforce.com	Customer Community Member (100 Members) Premier+ Success	204-1477PPS	$ 1,050.00	$ 1,012.87
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Premier Success	204-1648PS	$ 1,080.00	$ 1,041.81
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month (Partial Copy)	204-1653SBP	$ 1,120.00	$ 1,080.39
Salesforce.com	Partner Community Members - 10 Members Sandbox (Partial Copy)	204-1612SBP	$ 1,200.00	$ 1,157.56
Salesforce.com	Additional 10 Objects for Partner Community Members (10 Members)	204-1637	$ 1,200.00	$ 1,157.56
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month (Partial Copy)	204-1646SBP	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - Additional Database Contacts (10000)	204-1657	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - File Hosting (500MB)	204-1661	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - Inbound Marketing (SEO & Competitor)	204-1664	$ 1,200.00	$ 1,157.56
Salesforce.com	Customer Community Member (100 Members) Sandbox (Full Copy)	204-1477SBF	$ 1,260.00	$ 1,215.44
Salesforce.com	Customer Community Logins- 1000 Logins/Month Premier Success	204-1635PS	$ 1,350.00	$ 1,302.26
Salesforce.com	Customer Community Plus- 1000 Logins/Month Sanbox (Developer Pro)	204-1626SBD	$ 1,400.00	$ 1,350.49
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Premier+ Success	204-1653PPS	$ 1,400.00	$ 1,350.49
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Premier Success	204-1642PS	$ 1,440.00	$ 1,389.07
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members (Partial Copy)	204-1648SBP	$ 1,440.00	$ 1,389.07
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Sanbox (Developer Pro)	204-1649SBD	$ 1,440.00	$ 1,389.07
Salesforce.com	Partner Community Members - 10 Members Premier+ Success	204-1612PPS	$ 1,500.00	$ 1,446.95
Salesforce.com	Customer Community Logins- 5000 Logins/Month Sanbox (Developer Pro)	204-1636SBD	$ 1,500.00	$ 1,446.95
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Premier+ Success	204-1646PPS	$ 1,500.00	$ 1,446.95
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Sanbox (Developer Pro)	204-1650SBD	$ 1,620.00	$ 1,562.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Government Cloud	204-1653GC	$ 1,680.00	$ 1,620.59
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Sandbox (Full Copy)	204-1653SBF	$ 1,680.00	$ 1,620.59
Salesforce.com	Partner Community Members - 10 Members Government Cloud	204-1612GC	$ 1,800.00	$ 1,736.34
Salesforce.com	Partner Community Members - 10 Members Sandbox (Full Copy)	204-1612SBF	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Plus- 500 Members Sanbox (Developer Pro)	204-1620SBD	$ 1,800.00	$ 1,736.34

Salesforce.com	Customer Community Logins- 1000 Logins/Month (Partial Copy)	204-1635SBP	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Government Cloud	204-1646GC	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Sandbox (Full Copy)	204-1646SBF	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Premier+ Success	204-1648PPS	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Sanbox (Developer Pro)	204-1655SBD	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Member (500 Members) Premier Success	204-1478PS	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Logins (2000 logins/month) Premier Success	204-1482PS	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members (Partial Copy)	204-1642SBP	$ 1,920.00	$ 1,852.10
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month	204-1645	$ 1,920.00	$ 1,852.10
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Government Cloud	204-1648GC	$ 2,160.00	$ 2,083.61
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Sandbox (Full Copy)	204-1648SBF	$ 2,160.00	$ 2,083.61
Salesforce.com	Customer Community Logins- 1000 Logins/Month Premier+ Success	204-1635PPS	$ 2,250.00	$ 2,170.43
Salesforce.com	Customer Community Plus- 10 Members	204-1619	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Members- 2500 Members Sanbox (Developer Pro)	204-1632SBD	$ 2,400.00	$ 2,315.12
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Premier+ Success	204-1642PPS	$ 2,400.00	$ 2,315.12
Salesforce.com	Public Communities Page Views (1 million/month) Sanbox (Developer Pro)	204-1656SBD	$ 2,400.00	$ 2,315.12
Salesforce.com	Pardot- Database - Automation Rules (50)	204-1670	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Member (500 Members) Sandbox (Partial Copy)	204-1478SBP	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Partial Copy)	204-1482SBP	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Logins- 1000 Logins/Month Government Cloud	204-1635GC	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Logins- 1000 Logins/Month Sandbox (Full Copy)	204-1635SBF	$ 2,700.00	$ 2,604.51
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Premier Success	204-1654PS	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Developer Pro)	204-1479SBD	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Partial Copy)	204-1479SBP	$ 2,700.00	$ 2,604.51
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Premier Success	204-1640PS	$ 2,880.00	$ 2,778.15
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Government Cloud	204-1642GC	$ 2,880.00	$ 2,778.15
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Sandbox (Full Copy)	204-1642SBF	$ 2,880.00	$ 2,778.15
Salesforce.com	Customer Community Logins- 200 Logins/Month	204-1634	$ 3,000.00	$ 2,893.90
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Sanbox (Developer Pro)	204-1651SBD	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Member (500 Members) Premier+ Success	204-1478PPS	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Logins (2000 logins/month) Premier+ Success	204-1482PPS	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Developer Pro)	204-1483SBD	$ 3,000.00	$ 2,893.90
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Premier Success	204-1643PS	$ 3,060.00	$ 2,951.78
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month (Partial Copy)	204-1654SBP	$ 3,600.00	$ 3,472.69
Salesforce.com	Customer Community Member (500 Members) Sandbox (Full Copy)	204-1478SBF	$ 3,600.00	$ 3,472.69
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Full Copy)	204-1482SBF	$ 3,600.00	$ 3,472.69
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Partial Copy)	204-1640SBP	$ 3,840.00	$ 3,704.20
Salesforce.com	Pardot- Database - Quick Start (one time fee)	204-1671	$ 4,000.00	$ 3,858.54
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members (Partial Copy)	204-1643SBP	$ 4,080.00	$ 3,935.71
Salesforce.com	Customer Community Plus- 1000 Logins/Month Premier Success	204-1626PS	$ 4,200.00	$ 4,051.47
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Sanbox (Developer Pro)	204-1638SBD	$ 4,320.00	$ 4,167.22
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Premier Success	204-1649PS	$ 4,320.00	$ 4,167.22
Salesforce.com	Customer Community Plus- 5000 Logins/Month Sanbox (Developer Pro)	204-1627SBD	$ 4,500.00	$ 4,340.86
Salesforce.com	Customer Community Logins- 5000 Logins/Month Premier Success	204-1636PS	$ 4,500.00	$ 4,340.86
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Sanbox (Developer Pro)	204-1652SBD	$ 4,500.00	$ 4,340.86
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Premier+ Success	204-1654PPS	$ 4,500.00	$ 4,340.86
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Developer Pro)	204-1616SBD	$ 4,800.00	$ 4,630.25
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Premier+ Success	204-1640PPS	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Custom Object Intergration (4)	204-1658	$ 4,800.00	$ 4,630.25

Salesforce.com	Pardot- Database - API Access (100000/day)	204-1659	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Advanced Email Analytics	204-1660	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Advanced Dynamic Content	204-1662	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Google Adwords Integration	204-1665	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Social Profiles & Lookups	204-1667	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Expansion Pack	204-1669	$ 4,800.00	$ 4,630.25
Salesforce.com	BCC Email Compliance	204-1672	$ 4,800.00	$ 4,630.25
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Premier Success	204-1650PS	$ 4,860.00	$ 4,688.12
Salesforce.com	Customer Community Members- 10000 Members Sanbox (Developer Pro)	204-1633SBD	$ 5,100.00	$ 4,919.64
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Premier+ Success	204-1643PPS	$ 5,100.00	$ 4,919.64
Salesforce.com	Customer Community Plus- 500 Members Premier Success	204-1620PS	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Government Cloud	204-1654GC	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Sandbox (Full Copy)	204-1654SBF	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Premier Success	204-1655PS	$ 5,400.00	$ 5,209.03
Salesforce.com	Customer Community Plus- 1000 Logins/Month (Partial Copy)	204-1626SBP	$ 5,600.00	$ 5,401.95
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month	204-1653	$ 5,600.00	$ 5,401.95
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Government Cloud	204-1640GC	$ 5,760.00	$ 5,556.30
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Full Copy)	204-1640SBF	$ 5,760.00	$ 5,556.30
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members (Partial Copy)	204-1649SBP	$ 5,760.00	$ 5,556.30
Salesforce.com	Partner Community Members - 10 Members	204-1612	$ 6,000.00	$ 5,787.81
Salesforce.com	Customer Community Logins- 5000 Logins/Month (Partial Copy)	204-1636SBP	$ 6,000.00	$ 5,787.81
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month	204-1646	$ 6,000.00	$ 5,787.81
Salesforce.com	Pardot- Database - Dedicated IP	204-1663	$ 6,000.00	$ 5,787.81
Salesforce.com	Pardot- Database - Custom User Roles (Unlimited)	204-1666	$ 6,000.00	$ 5,787.81
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Developer Pro)	204-1484SBD	$ 6,000.00	$ 5,787.81
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Government Cloud	204-1643GC	$ 6,120.00	$ 5,903.56
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Sandbox (Full Copy)	204-1643SBF	$ 6,120.00	$ 5,903.56
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members (Partial Copy)	204-1650SBP	$ 6,480.00	$ 6,250.83
Salesforce.com	Customer Community Plus- 1000 Logins/Month Premier+ Success	204-1626PPS	$ 7,000.00	$ 6,752.44
Salesforce.com	Customer Community Plus- 500 Members (Partial Copy)	204-1620SBP	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Plus- 2500 Members Sanbox (Developer Pro)	204-1621SBD	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Members- 2500 Members Premier Success	204-1632PS	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members	204-1648	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Premier+ Success	204-1649PPS	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month (Partial Copy)	204-1655SBP	$ 7,200.00	$ 6,945.37
Salesforce.com	Public Communities Page Views (1 million/month) Premier Success	204-1656PS	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Logins- 5000 Logins/Month Premier+ Success	204-1636PPS	$ 7,500.00	$ 7,234.76
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Developer Pro)	204-1480SBD	$ 7,500.00	$ 7,234.76
Salesforce.com	Customer Community Plus- 5000 Members Sanbox (Developer Pro)	204-1622SBD	$ 8,100.00	$ 7,813.54
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Premier+ Success	204-1650PPS	$ 8,100.00	$ 7,813.54
Salesforce.com	Customer Community Member (5000 Members) Premier Success	204-1479PS	$ 8,100.00	$ 7,813.54
Salesforce.com	Customer Community Plus- 1000 Logins/Month Government Cloud	204-1626GC	$ 8,400.00	$ 8,102.93
Salesforce.com	Customer Community Plus- 1000 Logins/Month Sandbox (Full Copy)	204-1626SBF	$ 8,400.00	$ 8,102.93
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Government Cloud	204-1649GC	$ 8,640.00	$ 8,334.44
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Sandbox (Full Copy)	204-1649SBF	$ 8,640.00	$ 8,334.44
Salesforce.com	Customer Community Plus- 500 Members Premier+ Success	204-1620PPS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Plus- 20000 Logins/Month Sanbox (Developer Pro)	204-1628SBD	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins- 1000 Logins/Month	204-1635	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins- 5000 Logins/Month Government Cloud	204-1636GC	$ 9,000.00	$ 8,681.71

Salesforce.com	Customer Community Logins- 5000 Logins/Month Sandbox (Full Copy)	204-1636SBF	$ 9,000.00	$ 8,681.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Premier Success	204-1651PS	$ 9,000.00	$ 8,681.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Premier+ Success	204-1655PPS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins (20000 logins/month) Premier Success	204-1483PS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Members- 2500 Members (Partial Copy)	204-1632SBP	$ 9,600.00	$ 9,260.49
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members	204-1642	$ 9,600.00	$ 9,260.49
Salesforce.com	Public Communities Page Views (1 million/month) (Partial Copy)	204-1656SBP	$ 9,600.00	$ 9,260.49
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Government Cloud	204-1650GC	$ 9,720.00	$ 9,376.25
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Sandbox (Full Copy)	204-1650SBF	$ 9,720.00	$ 9,376.25
Salesforce.com	Customer Community Plus- 500 Members Government Cloud	204-1620GC	$ 10,800.00	$ 10,418.06
Salesforce.com	Customer Community Plus- 500 Members Sandbox (Full Copy)	204-1620SBF	$ 10,800.00	$ 10,418.06
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Government Cloud	204-1655GC	$ 10,800.00	$ 10,418.06
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Sandbox (Full Copy)	204-1655SBF	$ 10,800.00	$ 10,418.06
Salesforce.com	Customer Community Members- 2500 Members Premier+ Success	204-1632PPS	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Sanbox (Developer Pro)	204-1639SBD	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members (Partial Copy)	204-1651SBP	$ 12,000.00	$ 11,575.62
Salesforce.com	Public Communities Page Views (1 million/month) Premier+ Success	204-1656PPS	$ 12,000.00	$ 11,575.62
Salesforce.com	Pardot- Database - Phone Support	204-1668	$ 12,000.00	$ 11,575.62
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Partial Copy)	204-1483SBP	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Premier Success	204-1638PS	$ 12,960.00	$ 12,501.67
Salesforce.com	Customer Community Plus- 5000 Logins/Month Premier Success	204-1627PS	$ 13,500.00	$ 13,022.57
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Premier Success	204-1652PS	$ 13,500.00	$ 13,022.57
Salesforce.com	Customer Community Member (5000 Members) Premier+ Success	204-1479PPS	$ 13,500.00	$ 13,022.57
Salesforce.com	Heroku - 1000 Add On Credit	204-1611	$ 14,400.00	$ 13,890.74
Salesforce.com	Partner Community Logins- 2000 Logins/Month Premier Success	204-1616PS	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Members- 2500 Members Government Cloud	204-1632GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Members- 2500 Members Sandbox (Full Copy)	204-1632SBF	$ 14,400.00	$ 13,890.74
Salesforce.com	Public Communities Page Views (1 million/month) Government Cloud	204-1656GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Public Communities Page Views (1 million/month) Sandbox (Full Copy)	204-1656SBF	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Plus- 10000 Members Sanbox (Developer Pro)	204-1623SBD	$ 15,000.00	$ 14,469.52
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Premier+ Success	204-1651PPS	$ 15,000.00	$ 14,469.52
Salesforce.com	Customer Community Logins (20000 logins/month) Premier+ Success	204-1483PPS	$ 15,000.00	$ 14,469.52
Salesforce.com	Customer Community Members- 10000 Members Premier Success	204-1633PS	$ 15,300.00	$ 14,758.91
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Full Copy)	204-1479SBF	$ 16,200.00	$ 15,627.08
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) (Partial Copy)	204-1638SBP	$ 17,280.00	$ 16,668.89
Salesforce.com	Customer Community Plus- 5000 Logins/Month (Partial Copy)	204-1627SBP	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Government Cloud	204-1651GC	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Sandbox (Full Copy)	204-1651SBF	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members (Partial Copy)	204-1652SBP	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month	204-1654	$ 18,000.00	$ 17,363.43
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Full Copy)	204-1483SBF	$ 18,000.00	$ 17,363.43
Salesforce.com	Customer Community Plus- 5000 Members Premier Success	204-1622PS	$ 24,300.00	$ 23,440.62
Salesforce.com	Customer Community Members- 10000 Members Premier+ Success	204-1633PPS	$ 25,500.00	$ 24,598.19
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Government Cloud	204-1638GC	$ 25,920.00	$ 25,003.33
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Sandbox (Full Copy)	204-1638SBF	$ 25,920.00	$ 25,003.33
Salesforce.com	Customer Community Plus- 5000 Logins/Month Government Cloud	204-1627GC	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 5000 Logins/Month Sandbox (Full Copy)	204-1627SBF	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 20000 Logins/Month Premier Success	204-1628PS	$ 27,000.00	$ 26,045.14
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Government Cloud	204-1652GC	$ 27,000.00	$ 26,045.14

Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Sandbox (Full Copy)	204-1652SBF	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 1000 Logins/Month	204-1626	$ 28,000.00	$ 27,009.77
Salesforce.com	Partner Community Logins- 2000 Logins/Month Government Cloud	204-1616GC	$ 28,800.00	$ 27,781.48
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Full Copy)	204-1616SBF	$ 28,800.00	$ 27,781.48
Salesforce.com	Customer Community Plus- 2500 Members (Partial Copy)	204-1621SBP	$ 28,800.00	$ 27,781.48
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members	204-1649	$ 28,800.00	$ 27,781.48
Salesforce.com	Customer Community Logins- 5000 Logins/Month	204-1636	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Partial Copy)	204-1480SBP	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Developer Pro)	204-1481SBD	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Logins (100000 logins/month) Premier+ Success	204-1484PPS	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Developer Pro)	204-1485SBD	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Members- 10000 Members Government Cloud	204-1633GC	$ 30,600.00	$ 29,517.82
Salesforce.com	Customer Community Members- 10000 Members Sandbox (Full Copy)	204-1633SBF	$ 30,600.00	$ 29,517.82
Salesforce.com	Customer Community Plus- 5000 Members (Partial Copy)	204-1622SBP	$ 32,400.00	$ 31,254.17
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members	204-1650	$ 32,400.00	$ 31,254.17
Salesforce.com	Customer Community Plus- 500 Members	204-1620	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Plus- 2500 Members Premier+ Success	204-1621PPS	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Plus- 20000 Logins/Month (Partial Copy)	204-1628SBP	$ 36,000.00	$ 34,726.85
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Premier Success	204-1639PS	$ 36,000.00	$ 34,726.85
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month	204-1655	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Full Copy)	204-1484SBF	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Member (25000 Members) Premier+ Success	204-1480PPS	$ 37,500.00	$ 36,173.80
Salesforce.com	Customer Community Plus- 5000 Members Premier+ Success	204-1622PPS	$ 40,500.00	$ 39,067.71
Salesforce.com	Customer Community Plus- 2500 Members Government Cloud	204-1621GC	$ 43,200.00	$ 41,672.22
Salesforce.com	Customer Community Plus- 2500 Members Sandbox (Full Copy)	204-1621SBF	$ 43,200.00	$ 41,672.22
Salesforce.com	Customer Community Plus- 10000 Members Premier Success	204-1623PS	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Plus- 20000 Logins/Month Premier+ Success	204-1628PPS	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Full Copy)	204-1480SBF	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Members- 2500 Members	204-1632	$ 48,000.00	$ 46,302.47
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) (Partial Copy)	204-1639SBP	$ 48,000.00	$ 46,302.47
Salesforce.com	Public Communities Page Views (1 million/month)	204-1656	$ 48,000.00	$ 46,302.47
Salesforce.com	Customer Community Plus- 5000 Members Government Cloud	204-1622GC	$ 48,600.00	$ 46,881.25
Salesforce.com	Customer Community Plus- 5000 Members Sandbox (Full Copy)	204-1622SBF	$ 48,600.00	$ 46,881.25
Salesforce.com	Customer Community Plus- 20000 Logins/Month Government Cloud	204-1628GC	$ 54,000.00	$ 52,090.28
Salesforce.com	Customer Community Plus- 20000 Logins/Month Sandbox (Full Copy)	204-1628SBF	$ 54,000.00	$ 52,090.28
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Developer Pro)	204-1614SBD	$ 60,000.00	$ 57,878.09
Salesforce.com	Customer Community Plus- 10000 Members (Partial Copy)	204-1623SBP	$ 60,000.00	$ 57,878.09
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Premier+ Success	204-1639PPS	$ 60,000.00	$ 57,878.09
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members	204-1651	$ 60,000.00	$ 57,878.09
Salesforce.com	Partner Community Members- 5000 Members Premier Success	204-1613PS	$ 64,800.00	$ 62,508.33
Salesforce.com	Customer Community Plus- 25000 Members Premier Success	204-1624PS	$ 67,500.00	$ 65,112.85
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Government Cloud	204-1639GC	$ 72,000.00	$ 69,453.70
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Sandbox (Full Copy)	204-1639SBF	$ 72,000.00	$ 69,453.70
Salesforce.com	Customer Community Plus- 10000 Members Premier+ Success	204-1623PPS	$ 75,000.00	$ 72,347.61
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Partial Copy)	204-1613SBP	$ 86,400.00	$ 83,344.44
Salesforce.com	Additional 10 Objects for Partner Community Members (5000 Members)	204-1638	$ 86,400.00	$ 83,344.44
Salesforce.com	Customer Community Plus- 10000 Members Government Cloud	204-1623GC	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Plus- 10000 Members Sandbox (Full Copy)	204-1623SBF	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Plus- 25000 Members (Partial Copy)	204-1624SBP	$ 90,000.00	$ 86,817.13

Salesforce.com	Customer Community Plus- 5000 Logins/Month	204-1627	$ 90,000.00	$ 86,817.13
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members	204-1652	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Member (250000 Members) Premier Success	204-1481PS	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Logins (1000000 logins/month) Premier Success	204-1485PS	$ 90,000.00	$ 86,817.13
Salesforce.com	Partner Community Logins- 2000 Logins/Month	204-1616	$ 96,000.00	$ 92,604.94
Salesforce.com	Customer Community Members- 10000 Members	204-1633	$ 102,000.00	$ 98,392.75
Salesforce.com	Partner Community Members- 5000 Members Premier+ Success	204-1613PPS	$ 108,000.00	$ 104,180.55
Salesforce.com	Customer Community Plus- 25000 Members Premier+ Success	204-1624PPS	$ 112,500.00	$ 108,521.41
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Partial Copy)	204-1481SBP	$ 120,000.00	$ 115,756.17
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Partial Copy)	204-1485SBP	$ 120,000.00	$ 115,756.17
Salesforce.com	Partner Community Members- 5000 Members Government Cloud	204-1613GC	$ 129,600.00	$ 125,016.66
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Full Copy)	204-1613SBF	$ 129,600.00	$ 125,016.66
Salesforce.com	Customer Community Plus- 25000 Members Government Cloud	204-1624GC	$ 135,000.00	$ 130,225.69
Salesforce.com	Customer Community Plus- 25000 Members Sandbox (Full Copy)	204-1624SBF	$ 135,000.00	$ 130,225.69
Salesforce.com	Customer Community Plus- 2500 Members	204-1621	$ 144,000.00	$ 138,907.41
Salesforce.com	Customer Community Member (250000 Members) Premier+ Success	204-1481PPS	$ 150,000.00	$ 144,695.21
Salesforce.com	Customer Community Logins (1000000 logins/month) Premier+ Success	204-1485PPS	$ 150,000.00	$ 144,695.21
Salesforce.com	Customer Community Plus- 5000 Members	204-1622	$ 162,000.00	$ 156,270.83
Salesforce.com	Partner Community Members- 25000 Members Premier Success	204-1614PS	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Plus- 20000 Logins/Month	204-1628	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Full Copy)	204-1481SBF	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Full Copy)	204-1485SBF	$ 180,000.00	$ 173,634.26
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Partial Copy)	204-1614SBP	$ 240,000.00	$ 231,512.34
Salesforce.com	Additional 10 Objects for Partner Community Members (25000 Members)	204-1639	$ 240,000.00	$ 231,512.34
Salesforce.com	Partner Community Members- 25000 Members Premier+ Success	204-1614PPS	$ 300,000.00	$ 289,390.43
Salesforce.com	Partner Community Members Sandbox (20 Members)	204-1468SB	$ 2,520.00	$ 2,413.11
Salesforce.com	Partner Community Members Sandbox (100 Members)	204-1469SB	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Members Sandbox (500 Members)	204-1470SB	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Members Sandbox (10000 Members)	204-1472SB	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Members Premier Support (20 Members)	204-1468PS	$ 1,260.00	$ 1,206.55
Salesforce.com	Partner Community Members Premier Support (100 Members)	204-1469PS	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Members Premier Support (500 Members)	204-1470PS	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Members Premier Support+ (20 Members)	204-1468PPS	$ 2,100.00	$ 2,010.92
Salesforce.com	Partner Community Members Premier Support+ (100 Members)	204-1469PPS	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Members Premier Support+ (500 Members)	204-1470PPS	$ 24,000.00	$ 22,981.96
Salesforce.com	Customer Community Members Sandbox (500 Members)	204-1478SB	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members Sandbox (5000 Members)	204-1479SB	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Plus (20 Members) Premier Support	204-1563PS	$ 540.00	$ 516.88
Salesforce.com	Customer Community Plus (100 Members) Premier Support	204-1564PS	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier Support	204-1565PS	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier Support	204-1566PS	$ 7,200.00	$ 6,891.69
Salesforce.com	Customer Community Plus (20 Members) Premier+ Support	204-1563PPS	$ 900.00	$ 861.46
Salesforce.com	Customer Community Plus (100 Members) Premier+ Support	204-1564PPS	$ 3,000.00	$ 2,871.54
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier+ Support	204-1565PPS	$ 2,100.00	$ 2,010.08
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier+ Support	204-1566PPS	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (20 Members) Sandbox	204-1563SB	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members) Sandbox	204-1564SB	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month) Sandbox	204-1565SB	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month) Sandbox	204-1566SB	$ 14,400.00	$ 13,783.38

Salesforce.com	Lightning Connect (Price is per connection)	204-1674	$ 48,000.00	$ 46,302.47
Salesforce.com	Analytics Cloud - Additional Data Rows (100 Million)	204-1675	$ 48,000.00	$ 46,302.47
Salesforce.com	Analytics Cloud - Additional Data Rows (100 Million) Government Cloud	204-1675GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Analytics Cloud - Sales Wave Analytics App	204-1676	$ 900.00	$ 868.17
Salesforce.com	Customer Community Plus- 10000 Members	204-1623	$ 300,000.00	$ 289,390.43
Salesforce.com	Partner Community Members- 25000 Members Government Cloud	204-1614GC	$ 360,000.00	$ 347,268.51
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Full Copy)	204-1614SBF	$ 360,000.00	$ 347,268.51
Salesforce.com	Partner Community Members- 5000 Members	204-1613	$ 432,000.00	$ 416,722.22
Salesforce.com	Customer Community Plus- 25000 Members	204-1624	$ 450,000.00	$ 434,085.64
Salesforce.com	Partner Community Members- 25000 Members	204-1614	$ 1,200,000.00	$ 1,157,561.71
Salesforce.com	Customer Community Logins (100000 logins/month) Premier Success	204-1484PS	$ 18,000.00	$ 17,363.43
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Partial Copy)	204-1616SBP	$ 19,200.00	$ 18,520.99
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month	204-1640	$ 19,200.00	$ 18,520.99
Salesforce.com	Customer Community Members- 10000 Members (Partial Copy)	204-1633SBP	$ 20,400.00	$ 19,678.55
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members	204-1643	$ 20,400.00	$ 19,678.55
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Developer Pro)	204-1613SBD	$ 21,600.00	$ 20,836.11
Salesforce.com	Customer Community Plus- 2500 Members Premier Success	204-1621PS	$ 21,600.00	$ 20,836.11
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Premier+ Success	204-1638PPS	$ 21,600.00	$ 20,836.11
Salesforce.com	Customer Community Plus- 25000 Members Sanbox (Developer Pro)	204-1624SBD	$ 22,500.00	$ 21,704.28
Salesforce.com	Customer Community Plus- 5000 Logins/Month Premier+ Success	204-1627PPS	$ 22,500.00	$ 21,704.28
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Premier+ Success	204-1652PPS	$ 22,500.00	$ 21,704.28
Salesforce.com	Customer Community Member (25000 Members) Premier Success	204-1480PS	$ 22,500.00	$ 21,704.28
Salesforce.com	Partner Community Logins- 2000 Logins/Month Premier+ Success	204-1616PPS	$ 24,000.00	$ 23,151.23
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Partial Copy)	204-1484SBP	$ 24,000.00	$ 23,151.23
Salesforce.com	Partner Community Logins Premier Support (5000 Logins/Month)	204-1475PS	$ 36,000.00	$ 34,458.44
Salesforce.com	Partner Community Logins Sandbox (5000 Logins/Month)	204-1475SB	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins (20000 Logins/Month)	204-1476	$ 480,000.00	$ 459,445.84
Salesforce.com	Partner Community Logins (20000 Logins/Month) Government Cloud	204-1476GC	$ 144,000.00	$ 137,833.75
Salesforce.com	Partner Community Logins Premier Support (20000 Logins/Month)	204-1476PS	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins Sandbox (20000 Logins/Month)	204-1476SB	$ 144,000.00	$ 137,833.75
Salesforce.com	Customer Community Members (100 Members)	204-1477	$ 4,200.00	$ 4,020.15
Salesforce.com	Customer Community Members (100 Members) Government Cloud	204-1477GC	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Members Sandbox (100 Members)	204-1477SB	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Logins (100000 Logins/Month) Government Cloud	204-1484GC	$ 36,000.00	$ 34,458.44
Salesforce.com	Analytics Cloud - Sales Wave Analytics App Government Cloud	204-1676GC	$ 270.00	$ 260.45
Salesforce.com	Apex Debugger	204-1677	$ 18,000.00	$ 17,363.43
Salesforce.com	Apex Debugger	204-1677GC	$ 5,400.00	$ 5,209.03
Salesforce.com	Platform Cache	204-1678	$ 3,600.00	$ 3,472.69
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition	204-1679	$ 3,600.00	$ 3,472.69
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Government Cloud	204-1679GC	$ 1,080.00	$ 1,041.81
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Premier Success	204-1679PS	$ 540.00	$ 520.90
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Premier + Success	204-1679PPS	$ 900.00	$ 868.17
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Sandbox (Developer Pro)	204-1679SBD	$ 180.00	$ 173.63
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition (Sandbox Full Copy)	204-1679SBF	$ 1,080.00	$ 1,041.81
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition (Sandbox Partial Copy)	204-1679SBP	$ 720.00	$ 694.54
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition	204-1680	$ 5,400.00	$ 5,209.03
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Government Cloud	204-1680GC	$ 270.00	$ 260.45
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Premier Success	204-1680PS	$ 810.00	$ 781.35
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Premier + Success	204-1680PPS	$ 1,350.00	$ 1,302.26

Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Sandbox (Developer Pro)	204-1680SBD	$ 270.00	$ 260.45
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition (Sandbox Full Copy)	204-1680SBF	$ 1,620.00	$ 1,562.71
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition (Sandbox Partial Copy)	204-1680SBP	$ 270.00	$ 260.45
Salesforce.com	SOS	204-1681	$ 1,800.00	$ 1,736.34
Salesforce.com	Force.com App Bundle PXE	204-1529	$ 960.00	$ 919.28
Salesforce.com	Force.com App Bundle UE	204-1530	$ 960.00	$ 919.28
Salesforce.com	Force.com App Bundle UE Government Cloud	204-1530GC	$ 48.00	$ 45.94
Salesforce.com	Force.com Admin PXE	204-1531	$ 900.00	$ 861.82
Salesforce.com	Additional Scheduled Analytics Bundle (price is per org)	204-1532	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org)	204-1533	$ 3,000.00	$ 2,872.75
Salesforce.com	Company Community (add on for Force.com)	204-1534	$ 240.00	$ 229.82
Salesforce.com	Customer Community Plus (200 Logins/Month) Government Cloud	204-1565GC	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month)	204-1566	$ 48,000.00	$ 45,944.58
Salesforce.com	Customer Community Plus (2000 Logins/Month) Government Cloud	204-1566GC	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Plus (20 Members) Premier Support	204-1567	$ 540.00	$ 516.88
Salesforce.com	Customer Community Plus (100 Members) Premier Support	204-1568	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier Support	204-1569	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier Support	204-1570	$ 7,200.00	$ 6,891.69
Salesforce.com	Customer Community Plus (20 Members) Premier+ Support	204-1571	$ 900.00	$ 861.46
Salesforce.com	Customer Community Plus (100 Members) Premier+ Support	204-1572	$ 3,000.00	$ 2,871.54
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier+ Support	204-1573	$ 2,100.00	$ 2,010.08
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier+ Support	204-1574	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (20 Members) Sandbox	204-1575	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members) Sandbox	204-1576	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month) Sandbox	204-1577	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month) Sandbox	204-1578	$ 14,400.00	$ 13,783.38
Salesforce.com	Employee Community only	204-1579	$ 240.00	$ 229.72
Salesforce.com	Employee Community only Government Cloud	204-1579GC	$ 72.00	$ 68.92
Salesforce.com	Employee Help Desk only	204-1580	$ 60.00	$ 57.43
Salesforce.com	Employee Help Desk only Government Cloud	204-1580GC	$ 18.00	$ 17.23
Salesforce.com	Files Connect	204-1590	$ 84.00	$ 80.44
Salesforce.com	Sites Pageviews (1 Million/month) - (price is per org)	204-1591	$ 24,000.00	$ 22,981.96
Salesforce.com	Unlimited Apps Pack	204-1592	$ 900.00	$ 861.82
Salesforce.com	Desk.com - Standard	204-1593	$ 420.00	$ 402.18
Salesforce.com	Desk.com - Pro	204-1594	$ 840.00	$ 804.37
Salesforce.com	Desk.com - Business	204-1595	$ 1,320.00	$ 1,264.01
Salesforce.com	Desk.com - Flex Bundle 1 (20 hours)	204-1596	$ 360.00	$ 344.73
Salesforce.com	Desk.com - Flex Bundle 2 (50 hours)	204-1597	$ 780.00	$ 746.91
Salesforce.com	Desk.com - Flex Bundle 3 (100 hours)	204-1598	$ 1,380.00	$ 1,321.46
Salesforce.com	Desk.com - Flex Bundle 4 (250 hours)	204-1599	$ 3,000.00	$ 2,872.75
Salesforce.com	Desk.com - Flex Bundle 5 (500 hours)	204-1600	$ 5,100.00	$ 4,883.67
Salesforce.com	Desk.com - Portal SSL	204-1601	$ 348.00	$ 333.24
Salesforce.com	Desk - Configuration +	204-1602	$ 3,000.00	$ 2,872.75
Salesforce.com	Desk - Advanced	204-1603	$ 3,500.00	$ 3,351.54
Salesforce.com	Desk - Data Import	204-1604	$ 1,500.00	$ 1,436.37
Salesforce.com	External Identity (25000 Unique Users/month) 5	204-1605	$ 24,000.00	$ 22,981.96
Salesforce.com	External Identity (250000 Unique Users/month) 5	204-1606	$ 120,000.00	$ 114,909.82
Salesforce.com	External Identity (1000000 Unique Users/month) 5	204-1607	$ 200,000.00	$ 191,516.37
Salesforce.com	External Identity (5000000 Unique Users/month) 5	204-1608	$ 500,000.00	$ 478,790.93

SAP	SAP ByDesign Base Fee	8000340	$ 1,650.00	$ 1,468.50
SAP	SAP ByDesign Enterprise Private Edition	8000274	$ 16,500.00	$ 14,685.00
SAP	SAP ByDesign CRM Sales Team User	8000046	$ 87.00	$ 77.43
SAP	SAP ByDesign Project Management Team User	8002711	$ 87.00	$ 77.43
SAP	SAP By Design Standard Enterprise User	8000045	$ 146.00	$ 129.94
SAP	SAP ByDesign SCM Enterprise User	8000044	$ 197.00	$ 175.33
SAP	SAP ByDesign Standard Self-Service User	8000049	$ 17.00	$ 15.13
SAP	SAP ByDesign SCM Self-Service User	8000048	$ 24.00	$ 21.36
SAP	SAP ByDesign Project Mgt Self Service User	8000047	$ 24.00	$ 21.36
SAP	SAP ByDesign Localization Fee	8002712	$ 880.00	$ 783.20
SAP	SAP ByDesign Test Tenant	8002713	$ 1,155.00	$ 1,027.95
SAP	SAP ByDesign Additional Productive Tenant	8000275	$ 1,155.00	$ 1,027.95
SAP	SAP Cloud Applications Studio	8000570	$ 184.00	$ 163.76
SAP	SAP Communication Center by ANCILE, base	8002954	$ 18,370.00	$ 16,349.30
SAP	SAP Communication Center by ANCILE, user	8002955	$ 26.00	$ 23.14
SAP	SAP Assessment Mgmt by Questionmark	8002535-1	$ 2.67	$ 2.38
SAP	SAP Assessment Mgmt by Questionmark	8002535-2	$ 2.58	$ 2.30
SAP	SAP Assessment Mgmt by Questionmark	8002535-3	$ 2.48	$ 2.21
SAP	SAP Assessment Mgmt by Questionmark	8002535-4	$ 2.39	$ 2.13
SAP	SAP Assessment Mgmt by Questionmark	8002535-5	$ 2.29	$ 2.04
SAP	SAP Assessment Mgmt by Questionmark	8002535-6	$ 2.20	$ 1.96
SAP	SAP Assessment Mgmt by Questionmark	8002535-7	$ 2.10	$ 1.87
SAP	SAP Assessment Mgmt by Questionmark	8002535-8	$ 2.01	$ 1.79
SAP	SAP Assessment Mgmt by Questionmark	8002535-9	$ 1.91	$ 1.70
SAP	SAP Assessment Mgmt by Questionmark	8002535-10	$ 1.52	$ 1.35
SAP	SAP Assessment Mgmt by Questionmark	8002535-11	$ 1.44	$ 1.28
SAP	SAP SuccessFactors Perform & Reward Package	8003753-1	$ 107.00	$ 95.23
SAP	SAP SuccessFactors Perform & Reward Package	8003753-2	$ 96.00	$ 85.44
SAP	SAP SuccessFactors Perform & Reward Package	8003753-3	$ 79.00	$ 70.31
SAP	SAP SuccessFactors Perform & Reward Package	8003753-4	$ 67.00	$ 59.63
SAP	SAP SuccessFactors Perform & Reward Package	8003753-5	$ 58.00	$ 51.62
SAP	SAP SuccessFactors Perform & Reward Package	8003753-6	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Perform & Reward Package	8003753-7	$ 49.00	$ 43.61
SAP	SAP SuccessFactors Perform & Reward Package	8003753-8	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Perform & Reward Package	8003753-9	$ 45.00	$ 40.05
SAP	SAP SuccessFactors Perform & Reward Package	8003753-10	$ 43.00	$ 38.27
SAP	SAP SuccessFactors Talent Management Package	8003754-1	$ 239.00	$ 212.71
SAP	SAP SuccessFactors Talent Management Package	8003754-2	$ 219.00	$ 194.91
SAP	SAP SuccessFactors Talent Management Package	8003754-3	$ 191.00	$ 169.99
SAP	SAP SuccessFactors Talent Management Package	8003754-4	$ 190.00	$ 169.10
SAP	SAP SuccessFactors Talent Management Package	8003754-5	$ 169.00	$ 150.41
SAP	SAP SuccessFactors Talent Management Package	8003754-6	$ 148.00	$ 131.72
SAP	SAP SuccessFactors Talent Management Package	8003754-7	$ 135.00	$ 120.15
SAP	SAP SuccessFactors Talent Management Package	8003754-8	$ 123.00	$ 109.47
SAP	SAP SuccessFactors Talent Management Package	8003754-9	$ 113.00	$ 100.57
SAP	SAP SuccessFactors Talent Management Package	8003754-10	$ 103.00	$ 91.67
SAP	SAP SuccessFactors Talent Management Package	8003754-11	$ 95.00	$ 84.55
SAP	SAP SuccessFactors Advanced Learning Package	8003754-12	$ 95.00	$ 84.55
SAP	SAP SuccessFactors Advanced Learning Package	8003754-13	$ 86.00	$ 76.54

SAP	SAP SuccessFactors Advanced Learning Package	8003754-14	$ 77.00	$ 68.53
SAP	SAP SuccessFactors Advanced Learning Package	8003754-15	$ 69.00	$ 61.41
SAP	SAP SuccessFactors Advanced Learning Package	8003754-16	$ 60.00	$ 53.40
SAP	SAP SuccessFactors Advanced Learning Package	8003754-17	$ 53.00	$ 47.17
SAP	SAP SuccessFactors Advanced Learning Package	8003754-18	$ 48.00	$ 42.72
SAP	SAP SuccessFactors Advanced Learning Package	8003754-19	$ 44.00	$ 39.16
SAP	SAP SuccessFactors Advanced Learning Package	8003754-20	$ 40.00	$ 35.60
SAP	SAP SuccessFactors Advanced Learning Package	8003754-21	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-1	$ 527.00	$ 469.03
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-2	$ 497.00	$ 442.33
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-3	$ 433.00	$ 385.37
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-4	$ 415.00	$ 369.35
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-5	$ 367.00	$ 326.63
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-6	$ 323.00	$ 287.47
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-7	$ 292.00	$ 259.88
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-8	$ 263.00	$ 234.07
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-9	$ 245.00	$ 218.05
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-10	$ 226.00	$ 201.14
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-11	$ 211.00	$ 187.79
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-1	$ 543.00	$ 483.27
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-2	$ 511.00	$ 454.79
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-3	$ 445.00	$ 396.05
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-4	$ 427.00	$ 380.03
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-5	$ 377.00	$ 335.53
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-6	$ 333.00	$ 296.37
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-7	$ 300.00	$ 267.00
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-8	$ 270.00	$ 240.30
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-9	$ 252.00	$ 224.28
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-10	$ 232.00	$ 206.48
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-11	$ 217.00	$ 193.13
SAP	SF-Perform & Reward Bundle for Small Business	8000720-1	$ 85.00	$ 75.65
SAP	SF-Perform & Reward Bundle for Small Business	8000720-2	$ 66.00	$ 58.74
SAP	SF-Perform & Reward Bundle for Small Business	8000720-3	$ 56.00	$ 49.84
SAP	SF-Perform & Reward Bundle for Small Business	8000720-4	$ 47.00	$ 41.83
SAP	SF-Perform & Reward Bundle for Small Business	8000720-5	$ 33.00	$ 29.37
SAP	SF-Perform & Reward Bundle for Small Business	8000720-6	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Performance & Goals	8003776-1	$ 68.00	$ 60.52
SAP	SAP SuccessFactors Performance & Goals	8003776-2	$ 61.00	$ 54.29
SAP	SAP SuccessFactors Performance & Goals	8003776-3	$ 50.00	$ 44.50
SAP	SAP SuccessFactors Performance & Goals	8003776-4	$ 43.00	$ 38.27
SAP	SAP SuccessFactors Performance & Goals	8003776-5	$ 37.00	$ 32.93
SAP	SAP SuccessFactors Performance & Goals	8003776-6	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Performance & Goals	8003776-7	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Performance & Goals	8003776-8	$ 30.00	$ 26.70
SAP	SAP SuccessFactors Performance & Goals	8003776-9	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Performance & Goals	8003776-10	$ 27.00	$ 24.03
SAP	SAP SuccessFactors Compensation	8003773-1	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Compensation	8003773-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Compensation	8003773-3	$ 28.00	$ 24.92

SAP	SAP SuccessFactors Compensation	8003773-4	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Compensation	8003773-5	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Compensation	8003773-6	$ 19.00	$ 16.91
SAP	SAP SuccessFactors Compensation	8003773-7	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Compensation	8003773-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Compensation	8003773-9	$ 16.00	$ 14.24
SAP	SAP SuccessFactors Compensation	8003773-10	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Succession & Development	8003774-1	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Succession & Development	8003774-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Succession & Development	8003774-3	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Succession & Development	8003774-4	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Succession & Development	8003774-5	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Succession & Development	8003774-6	$ 19.00	$ 16.91
SAP	SAP SuccessFactors Succession & Development	8003774-7	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Succession & Development	8003774-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Succession & Development	8003774-9	$ 16.00	$ 14.24
SAP	SAP SuccessFactors Succession & Development	8003774-10	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-1	$ 112.00	$ 99.68
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-2	$ 101.00	$ 89.89
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-3	$ 83.00	$ 73.87
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-4	$ 71.00	$ 63.19
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-5	$ 61.00	$ 54.29
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-6	$ 55.00	$ 48.95
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-7	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-8	$ 49.00	$ 43.61
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-9	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-10	$ 45.00	$ 40.05
SAP	SAP SuccessFactors Workforce Analytics	8003771-1	$ 118.00	$ 105.02
SAP	SAP SuccessFactors Workforce Analytics	8003771-2	$ 106.00	$ 94.34
SAP	SAP SuccessFactors Workforce Analytics	8003771-3	$ 94.00	$ 83.66
SAP	SAP SuccessFactors Workforce Analytics	8003771-4	$ 85.00	$ 75.65
SAP	SAP SuccessFactors Workforce Analytics	8003771-5	$ 77.00	$ 68.53
SAP	SAP SuccessFactors Workforce Analytics	8003771-6	$ 68.00	$ 60.52
SAP	SAP SuccessFactors Workforce Analytics	8003771-7	$ 59.00	$ 52.51
SAP	SAP SuccessFactors Workforce Analytics	8003771-8	$ 55.00	$ 48.95
SAP	SAP SuccessFactors Workforce Analytics	8003771-9	$ 51.00	$ 45.39
SAP	SAP SuccessFactors Workforce Analytics	8003771-10	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Workforce Planning	8003772-1	$ 59.00	$ 52.51
SAP	SAP SuccessFactors Workforce Planning	8003772-2	$ 53.00	$ 47.17
SAP	SAP SuccessFactors Workforce Planning	8003772-3	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Workforce Planning	8003772-4	$ 42.00	$ 37.38
SAP	SAP SuccessFactors Workforce Planning	8003772-5	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Workforce Planning	8003772-6	$ 34.00	$ 30.26
SAP	SAP SuccessFactors Workforce Planning	8003772-7	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Workforce Planning	8003772-8	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Workforce Planning	8003772-9	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Workforce Planning	8003772-10	$ 24.00	$ 21.36
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-1	$ 177.00	$ 157.53
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-2	$ 159.00	$ 141.51

SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-3	$ 141.00	$ 125.49
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-4	$ 127.00	$ 113.03
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-5	$ 115.00	$ 102.35
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-6	$ 102.00	$ 90.78
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-7	$ 88.00	$ 78.32
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-8	$ 83.00	$ 73.87
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-9	$ 76.00	$ 67.64
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-10	$ 71.00	$ 63.19
SAP	SF-Limited Active Users - Learning	8000603-1	$ 19.00	$ 16.91
SAP	SF-Limited Active Users - Learning	8000603-2	$ 18.00	$ 16.02
SAP	SF-Limited Active Users - Learning	8000603-3	$ 17.00	$ 15.13
SAP	SF-Limited Active Users - Learning	8000603-4	$ 16.00	$ 14.24
SAP	SF-Limited Active Users - Learning	8000603-5	$ 14.00	$ 12.46
SAP	SF-Limited Active Users - Learning	8000603-6	$ 13.00	$ 11.57
SAP	SF-Limited Active Users - Learning	8000603-7	$ 11.00	$ 9.79
SAP	SF-Limited Active Users - Learning	8000603-8	$ 9.30	$ 8.28
SAP	SF-Limited Active Users - Learning	8000603-9	$ 7.99	$ 7.11
SAP	SF-Limited Active Users - Learning	8000603-10	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Learning	8003763-1	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Learning	8003763-2	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Learning	8003763-3	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Learning	8003763-4	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Learning	8003763-5	$ 22.00	$ 19.58
SAP	SAP SuccessFactors Learning	8003763-6	$ 20.00	$ 17.80
SAP	SAP SuccessFactors Learning	8003763-7	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Learning	8003763-8	$ 14.00	$ 12.46
SAP	SAP SuccessFactors Learning	8003763-9	$ 12.00	$ 10.68
SAP	SAP SuccessFactors Learning	8003763-10	$ 11.00	$ 9.79
SAP	SF-Transactional Active Users - Learning	8000730-1	$ 9.40	$ 8.37
SAP	SF-Transactional Active Users - Learning	8000730-2	$ 5.41	$ 4.81
SAP	SF-Transactional Active Users - Learning	8000730-3	$ 5.13	$ 4.57
SAP	SF-Transactional Active Users - Learning	8000730-4	$ 4.62	$ 4.11
SAP	SF-Transactional Active Users - Learning	8000730-5	$ 4.15	$ 3.69
SAP	SF-Transactional Active Users - Learning	8000730-6	$ 3.75	$ 3.34
SAP	SF-Transactional Active Users - Learning	8000730-7	$ 3.37	$ 3.00
SAP	SF-Transactional Active Users - Learning	8000730-8	$ 3.04	$ 2.71
SAP	SF-Transactional Active Users - Learning	8000730-9	$ 2.73	$ 2.43
SAP	SF-Transactional Active Users - Learning	8000730-10	$ 2.45	$ 2.18
SAP	SF-External Active Users - Learning	8000665-1	$ 19.00	$ 16.91
SAP	SF-External Active Users - Learning	8000665-2	$ 18.00	$ 16.02
SAP	SF-External Active Users - Learning	8000665-3	$ 17.00	$ 15.13
SAP	SF-External Active Users - Learning	8000665-4	$ 16.00	$ 14.24
SAP	SF-External Active Users - Learning	8000665-5	$ 14.00	$ 12.46
SAP	SF-External Active Users - Learning	8000665-6	$ 13.00	$ 11.57
SAP	SF-External Active Users - Learning	8000665-7	$ 11.00	$ 9.79
SAP	SF-External Active Users - Learning	8000665-8	$ 9.30	$ 8.28
SAP	SF-External Active Users - Learning	8000665-9	$ 7.99	$ 7.11
SAP	SF-External Active Users - Learning	8000665-10	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Employee Central Payroll	8000773-1	$ 113.00	$ 100.57

SAP	SAP SuccessFactors Employee Central Payroll	8000773-2	$ 86.00	$ 76.54
SAP	SAP SuccessFactors Employee Central Payroll	8000773-3	$ 63.00	$ 56.07
SAP	SAP SuccessFactors Employee Central Payroll	8000773-4	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Employee Central Payroll	8000773-5	$ 44.00	$ 39.16
SAP	SAP SuccessFactors Employee Central Payroll	8000773-6	$ 37.00	$ 32.93
SAP	SAP SuccessFactors Employee Central Payroll	8000773-7	$ 32.00	$ 28.48
SAP	SAP SuccessFactors Employee Central Payroll	8000773-8	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Employee Central Payroll	8000773-9	$ 23.00	$ 20.47
SAP	SAP SuccessFactors Onboarding	8003775-1	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Onboarding	8003775-2	$ 14.00	$ 12.46
SAP	SAP SuccessFactors Onboarding	8003775-3	$ 12.00	$ 10.68
SAP	SAP SuccessFactors Onboarding	8003775-4	$ 11.00	$ 9.79
SAP	SAP SuccessFactors Onboarding	8003775-5	$ 9.02	$ 8.03
SAP	SAP SuccessFactors Onboarding	8003775-6	$ 7.98	$ 7.10
SAP	SAP SuccessFactors Onboarding	8003775-7	$ 7.52	$ 6.69
SAP	SAP SuccessFactors Onboarding	8003775-8	$ 7.06	$ 6.28
SAP	SAP SuccessFactors Onboarding	8003775-9	$ 6.45	$ 5.74
SAP	SAP SuccessFactors Onboarding	8003775-10	$ 6.02	$ 5.36
SAP	SAP SuccessFactors Recruiting	8003765-1	$ 36.00	$ 32.04
SAP	SAP SuccessFactors Recruiting	8003765-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Recruiting	8003765-3	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Recruiting	8003765-4	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Recruiting	8003765-5	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Recruiting	8003765-6	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Recruiting	8003765-7	$ 22.00	$ 19.58
SAP	SAP SuccessFactors Recruiting	8003765-8	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Recruiting	8003765-9	$ 15.00	$ 13.35
SAP	SAP Success Factors Recruiting Marketing	8003766-1	$ 26.00	$ 23.14
SAP	SAP Success Factors Recruiting Marketing	8003766-2	$ 25.00	$ 22.25
SAP	SAP Success Factors Recruiting Marketing	8003766-3	$ 25.00	$ 22.25
SAP	SAP Success Factors Recruiting Marketing	8003766-4	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Marketing	8003766-5	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Marketing	8003766-6	$ 23.00	$ 20.47
SAP	SAP Success Factors Recruiting Marketing	8003766-7	$ 22.00	$ 19.58
SAP	SAP Success Factors Recruiting Marketing	8003766-8	$ 21.00	$ 18.69
SAP	SAP Success Factors Recruiting Marketing	8003766-9	$ 19.00	$ 16.91
SAP	SAP Success Factors Recruiting Marketing	8003766-10	$ 16.00	$ 14.24
SAP	SAP Success Factors Recruiting Marketing	8003766-11	$ 13.00	$ 11.57
SAP	SAP Success Factors Recruiting Marketing	8003766-12	$ 10.00	$ 8.90
SAP	SAP SuccessFactors Learning Analytics	8000986-1	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Learning Analytics	8000986-2	$ 7.06	$ 6.28
SAP	SAP SuccessFactors Learning Analytics	8000986-3	$ 6.85	$ 6.10
SAP	SAP SuccessFactors Learning Analytics	8000986-4	$ 6.54	$ 5.82
SAP	SAP SuccessFactors Learning Analytics	8000986-5	$ 5.80	$ 5.16
SAP	SAP SuccessFactors Learning Analytics	8000986-6	$ 5.21	$ 4.64
SAP	SAP SuccessFactors Learning Analytics	8000986-7	$ 4.47	$ 3.98
SAP	SAP SuccessFactors Learning Analytics	8000986-8	$ 3.71	$ 3.30
SAP	SAP SuccessFactors Learning Analytics	8000986-9	$ 3.20	$ 2.85
SAP	SAP SuccessFactors Learning Analytics	8000986-10	$ 2.97	$ 2.64

SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-1	$ 56.00	$ 49.84
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-2	$ 51.00	$ 45.39
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-3	$ 42.00	$ 37.38
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-4	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-5	$ 30.00	$ 26.70
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-6	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-7	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-8	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-9	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-10	$ 22.00	$ 19.58
SAP	SF - Activity Based Users - Learning	8000361-1	$ 117.00	$ 104.13
SAP	SF - Activity Based Users - Learning	8000361-2	$ 59.00	$ 52.51
SAP	SF - Activity Based Users - Learning	8000361-3	$ 58.00	$ 51.62
SAP	SF - Activity Based Users - Learning	8000361-4	$ 58.00	$ 51.62
SAP	SF - Activity Based Users - Learning	8000361-5	$ 56.00	$ 49.84
SAP	SF - Activity Based Users - Learning	8000361-6	$ 53.00	$ 47.17
SAP	SF - Activity Based Users - Learning	8000361-7	$ 50.00	$ 44.50
SAP	SF - Activity Based Users - Learning	8000361-8	$ 46.00	$ 40.94
SAP	SF - Activity Based Users - Learning	8000361-9	$ 39.00	$ 34.71
SAP	SF - Activity Based Users - Learning	8000361-10	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Validated Learning	8003764-1	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Validated Learning	8003764-2	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Validated Learning	8003764-3	$ 32.00	$ 28.48
SAP	SAP SuccessFactors Validated Learning	8003764-4	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Validated Learning	8003764-5	$ 27.00	$ 24.03
SAP	SAP SuccessFactors Validated Learning	8003764-6	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Validated Learning	8003764-7	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Validated Learning	8003764-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Validated Learning	8003764-9	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Validated Learning	8003764-10	$ 14.00	$ 12.46
SAP	SAP Success Factors Recruiting Management	8003767-1	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Management	8003767-2	$ 23.00	$ 20.47
SAP	SAP Success Factors Recruiting Management	8003767-3	$ 22.00	$ 19.58
SAP	SAP Success Factors Recruiting Management	8003767-4	$ 21.00	$ 18.69
SAP	SAP Success Factors Recruiting Management	8003767-5	$ 20.00	$ 17.80
SAP	SAP Success Factors Recruiting Management	8003767-6	$ 19.00	$ 16.91
SAP	SAP Success Factors Recruiting Management	8003767-7	$ 18.00	$ 16.02
SAP	SAP Success Factors Recruiting Management	8003767-8	$ 17.00	$ 15.13
SAP	SAP Success Factors Recruiting Management	8003767-9	$ 15.00	$ 13.35
SAP	SAP Success Factors Recruiting Management	8003767-10	$ 13.00	$ 11.57
SAP	SAP Success Factors Recruiting Management	8003767-11	$ 11.00	$ 9.79
SAP	SAP Success Factors Recruiting Management	8003767-12	$ 9.40	$ 8.37
SAP	SF-Foundation Product	8000368-1	$ 18.00	$ 16.02
SAP	SF-Foundation Product	8000368-2	$ 16.00	$ 14.24
SAP	SF-Foundation Product	8000368-3	$ 13.00	$ 11.57
SAP	SF-Foundation Product	8000368-4	$ 11.00	$ 9.79
SAP	SF-Foundation Product	8000368-5	$ 9.49	$ 8.45
SAP	SF-Foundation Product	8000368-6	$ 8.61	$ 7.66
SAP	SF-Foundation Product	8000368-7	$ 8.08	$ 7.19

SAP	SF-Foundation Product	8000368-8	$ 7.73	$ 6.88
SAP	SF-Foundation Product	8000368-9	$ 7.38	$ 6.57
SAP	SF-Foundation Product	8000368-10	$ 7.02	$ 6.25
SAP	SF-Skills Content Library	8000728-1	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-2	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-3	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-4	$ 13.00	$ 11.57
SAP	SF-Skills Content Library	8000728-5	$ 12.00	$ 10.68
SAP	SF-Skills Content Library	8000728-6	$ 12.00	$ 10.68
SAP	SF-Skills Content Library	8000728-7	$ 8.81	$ 7.84
SAP	SF-Skills Content Library	8000728-8	$ 7.05	$ 6.27
SAP	SF-Skills Content Library	8000728-9	$ 6.26	$ 5.57
SAP	SF-Skills Content Library	8000728-10	$ 3.76	$ 3.35
SAP	SF-Skills Content Library	8000728-11	$ 2.35	$ 2.09
SAP	SF-Skills Content Library	8000728-12	$ 2.12	$ 1.89
SAP	SF-Additional Instances-Test	8003622	$ 9,398.00	$ 8,364.22
SAP	SF-Additional Instances-Production	8003623	$ 9,398.00	$ 8,364.22
SAP	BOOMI - Integration for Recruiting	8000943	$ 7,049.00	$ 6,273.61
SAP	Data Center Migration	8000988	$ 9,398.00	$ 8,364.22
SAP	SF-Attachment Storage Fee	8000374	$ 1.88	$ 1.67
SAP	SF-Visual Publisher	8000725	$ 14,097.00	$ 12,546.33
SAP	SF-BOOMI : Professional Edition Package	8000513	$ 12,405.00	$ 11,040.45
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, base edition	8003951	$ 1.10	$ 0.98
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, standard edition	8003952	$ 3.30	$ 2.94
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, enterprise edition	8003953	$ 11.00	$ 9.79
SAP	SAP SuccessFactors Disaster Recovery, enhanced option	8003778	$ 0.24	$ 0.24
SAP	SAP Jam Collaboration, advanced edition	8004154-1	$ 2.35	$ 2.09
SAP	SAP Jam Collaboration, advanced edition	8004154-2	$ 2.11	$ 1.88
SAP	SAP Jam Collaboration, advanced edition	8004154-3	$ 1.88	$ 1.67
SAP	SAP Jam Collaboration, advanced edition	8004154-4	$ 1.66	$ 1.48
SAP	SAP Jam Collaboration, advanced edition	8004154-5	$ 1.42	$ 1.26
SAP	SAP Jam Collaboration, advanced edition	8004154-6	$ 1.24	$ 1.10
SAP	SAP Jam Collaboration, advanced edition	8004154-7	$ 1.17	$ 1.04
SAP	SAP Jam Collaboration, advanced edition	8004154-8	$ 1.10	$ 0.98
SAP	SAP Jam Collaboration, advanced edition	8004154-9	$ 1.00	$ 0.89
SAP	SAP Jam Collaboration, advanced edition	8004154-10	$ 0.94	$ 0.84
SAP	SAP Jam Collaboration, advanced plus edition	8004155-1	$ 5.64	$ 5.02
SAP	SAP Jam Collaboration, advanced plus edition	8004155-2	$ 4.51	$ 4.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-3	$ 3.95	$ 3.52
SAP	SAP Jam Collaboration, advanced plus edition	8004155-4	$ 3.38	$ 3.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-5	$ 2.82	$ 2.51
SAP	SAP Jam Collaboration, advanced plus edition	8004155-6	$ 2.26	$ 2.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-7	$ 1.69	$ 1.50
SAP	SAP Jam Collaboration, advanced plus edition	8004155-8	$ 1.41	$ 1.25
SAP	SAP Jam Collaboration, enterprise edition	8004156-1	$ 14.00	$ 12.46
SAP	SAP Jam Collaboration, enterprise edition	8004156-2	$ 11.00	$ 9.79
SAP	SAP Jam Collaboration, enterprise edition	8004156-3	$ 9.87	$ 8.78
SAP	SAP Jam Collaboration, enterprise edition	8004156-4	$ 8.46	$ 7.53
SAP	SAP Jam Collaboration, enterprise edition	8004156-5	$ 7.05	$ 6.27

SAP	SAP Jam Collaboration, enterprise edition	8004156-6	$ 5.64	$ 5.02
SAP	SAP Jam Collaboration, enterprise edition	8004156-7	$ 4.23	$ 3.76
SAP	SAP Jam Collaboration, enterprise edition	8004156-8	$ 3.53	$ 3.14
SAP	SAP Jam Collaboration, external user	8000653-1	$ 3.76	$ 3.35
SAP	SAP Jam Collaboration, external user	8000653-2	$ 3.01	$ 2.68
SAP	SAP Jam Collaboration, external user	8000653-3	$ 2.63	$ 2.34
SAP	SAP Jam Collaboration, external user	8000653-4	$ 2.26	$ 2.01
SAP	SAP Jam Collaboration, external user	8000653-5	$ 1.88	$ 1.67
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-1	$ 4.45	$ 3.96
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-2	$ 3.56	$ 3.17
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-3	$ 3.11	$ 2.77
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-4	$ 2.67	$ 2.38
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-5	$ 2.22	$ 1.98
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-6	$ 1.78	$ 1.58
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-7	$ 1.33	$ 1.18
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-8	$ 1.12	$ 1.00
SAP	SAP Jam Collaboration, data storage add-on	8000654	$ 235.00	$ 209.15
SAP	SAP SuccessFactors Learning, content storage add-on	8003445	$ 1,400.00	$ 1,246.00
SAP	SAP SuccessFactors Learning, content bandwidth add-on	8003446	$ 570.00	$ 507.30
SAP	SF-Addit'l ATS To Extract For Analytics	8000381	$ 6,000.00	$ 5,340.00
SAP	SF-Site Scrape for Addit'l ATS Instances	8000382	$ 6,000.00	$ 5,340.00
SAP	SF-BOOMI: Add On Prod Use Connection	8000768	$ 3,000.00	$ 2,670.00
SAP	SF-BOOMI: Add On Test Use Connection	8000769	$ 1,500.00	$ 1,335.00
SAP	SAP US Benefits Eligible User	8003532-1	$ 152.00	$ 135.28
SAP	SAP US Benefits Eligible User	8003532-2	$ 138.00	$ 122.82
SAP	SAP US Benefits Eligible User	8003532-3	$ 132.00	$ 117.48
SAP	SAP US Benefits Eligible User	8003532-4	$ 126.00	$ 112.14
SAP	SAP US Benefits Eligible User	8003532-5	$ 113.00	$ 100.57
SAP	SAP US Benefits Eligible User	8003532-6	$ 99.00	$ 88.11
SAP	SAP US Benefits Non-Eligible User	8003533	$ 41.00	$ 36.49
SAP	SAP US Benefits Non-Std Interface User	8003534	$ 27.00	$ 24.03
SAP	SAP Time & Attendance Management by WFS	8003956-1	$ 115.50	$ 102.80
SAP	SAP Time & Attendance Management by WFS	8003956-2	$ 99.00	$ 88.11
SAP	SAP Time & Attendance Management by WFS	8003956-3	$ 88.00	$ 78.32
SAP	SAP Time & Attendance Management by WFS	8003956-4	$ 82.50	$ 73.43
SAP	SAP Time & Attendance Management by WFS	8003956-5	$ 77.00	$ 68.53
SAP	SAP Time & Attendance Management by WFS	8003956-6	$ 55.00	$ 48.95
SAP	SAP Time & Attendance Mgmt. for SME by WFS	8003956-7	$ 121,000.00	$ 107,690.00
SAP	SAP Time & Attendance by WFS Adnl Instance	8003958	$ 22.00	$ 19.58
SAP	SAP Product Stewardship Network - product compliance	8003360-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - product compliance	8003360-2	$ 2,200.00	$ 1,958.00
SAP	SAP Product Stewardship Network - product compliance	8003360-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - product compliance	8003360-4	$ 1,375.00	$ 1,223.75
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-2	$ 2,200.00	$ 1,958.00
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-4	$ 1,375.00	$ 1,223.75
SAP	SAP Product Stewardship Network - conflict minerals	8003361-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - conflict minerals	8003361-2	$ 2,200.00	$ 1,958.00

SAP	SAP Product Stewardship Network - conflict minerals	8003361-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - conflict minerals	8003361-4	$ 1,375.00	$ 1,223.75
SAP	Ariba Sourcing Professional	8000641-1	$ 630.00	$ 560.70
SAP	Ariba Sourcing Professional	8000641-2	$ 430.00	$ 382.70
SAP	Ariba Sourcing Professional	8000641-3	$ 270.00	$ 240.30
SAP	Ariba Sourcing Professional	8000641-4	$ 250.00	$ 222.50
SAP	Ariba Sourcing Professional	8000641-5	$ 230.00	$ 204.70
SAP	Ariba Contract Management Professional	8000625-1	$ 520.00	$ 462.80
SAP	Ariba Contract Management Professional	8000625-2	$ 400.00	$ 356.00
SAP	Ariba Contract Management Professional	8000625-3	$ 270.00	$ 240.30
SAP	Ariba Contract Management Professional	8000625-4	$ 200.00	$ 178.00
SAP	Ariba Contract Management Professional	8000625-5	$ 170.00	$ 151.30
SAP	Ariba Open Invoice Conversion Services	8002538	$ 0.30	$ 0.27
SAP	Ariba Additional Storage	8003324	$ 100.00	$ 89.00
SAP	SAP Predictive Maintenance and Service, measurements	8003165-1	$ 275.00	$ 244.75
SAP	SAP Predictive Maintenance and Service, measurements	8003165-2	$ 165.00	$ 146.85
SAP	SAP Predictive Maintenance and Service, measurements	8003165-3	$ 132.00	$ 117.48
SAP	SAP Predictive Maintenance and Service, measurements	8003165-4	$ 99.00	$ 88.11
SAP	SAP Predictive Maintenance and Service, measurements	8003165-5	$ 77.00	$ 68.53
SAP	SAP Predictive Maintenance and Service, devices	8003166	$ 33.00	$ 29.37
SAP	SAP Predictive Maintenance and Service, historic storage provisioning	8003167	$ 6,160.00	$ 5,482.40
SAP	SAP Predictive Maintenance and Service, additional historic measurements	8003168	$ 5.50	$ 4.90
SAP	SAP Predictive Maintenance and Service, Vibration Analysis add-on	8004025	$ 1.65	$ 1.47
SAP	SAP Innovation Management, cloud edition - Base Package	8003962	$ 55,000.00	$ 48,950.00
SAP	SAP Innovation Management, cloud edition	8003960-1	$ 39.00	$ 34.71
SAP	SAP Innovation Management, cloud edition	8003960-2	$ 28.00	$ 24.92
SAP	SAP Innovation Management, cloud edition	8003960-3	$ 11.00	$ 9.79
SAP	SAP Innovation Management, cloud edition - Additional Storage	8003963	$ 11.00	$ 9.79
SAP	Cloud for Product Stewardship: Basic Layer	8003959-1	$ 9,900.00	$ 8,811.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-2	$ 44,000.00	$ 39,160.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-3	$ 82,500.00	$ 73,425.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-4	$ 132,000.00	$ 117,480.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-5	$ 275,000.00	$ 244,750.00
SAP	SAP Cloud for Sales, User	8001003	$ 105.00	$ 93.45
SAP	SAP Cloud for Sales, service option	8003187	$ 55.00	$ 48.95
SAP	SAP Cloud for Service, User	8001004	$ 105.00	$ 93.45
SAP	SAP Cloud for Service, sales option	8003188	$ 55.00	$ 48.95
SAP	SAP Cloud for Social Engagement, User	8001005	$ 165.00	$ 146.85
SAP	SAP Cloud for Customer, Advanced User Option	8001006	$ 17.00	$ 15.13
SAP	SAP Cloud for Customer, B2B Industry User Option	8001007	$ 17.00	$ 15.13
SAP	SAP Cloud for Customer, Test Tenant	8000567	$ 11,000.00	$ 9,790.00
SAP	SAP Cloud for Customer, Additional Storage	8000568	$ 5.50	$ 4.90
SAP	SAP Cloud for Customer, Private Edition	8000981	$ 16,500.00	$ 14,685.00
SAP	SAP Cloud for Customer, enhanced package	8003185	$ 176.00	$ 156.64
SAP	SAP Cloud for Customer, limited package	8003186	$ 55.00	$ 48.95
SAP	SAP Cloud for Customer, Edge edition	8003938	$ 32.00	$ 28.48
SAP	SAP Cloud for Customer, enterprise edition	8003948	$ 219.00	$ 194.91
SAP	SAP Contact Center, e-channel, cloud ed.	8001016	$ 66.00	$ 58.74
SAP	SAP Contact Center, voice, cloud ed.	8001017	$ 121.00	$ 107.69

SAP	SAP Knowledge Central by Mindtouch-User	8003084	$ 17.00	$ 15.13
SAP	SAP Knowledge Central by Mindtouch-Ext Srv	8003085	$ 16,500.00	$ 14,685.00
SAP	SAP Knowledge Central by Mindtouch-Base	8003086	$ 4,400.00	$ 3,916.00
SAP	SAP Real-Time Communicator by GENBAND	8004033	$ 6.60	$ 5.87
SAP	SAP HANA Cloud Portal, Cloud for Customer Edition	8000793	$ 0.20	$ 0.20
SAP	SAP HANA Cloud Platform, extension package for SAP Cloud for Customer, standard edition	8003949	$ 17.00	$ 15.13
SAP	SAP HANA Cloud Platform, extension package for SAP Cloud for Customer, premium edition	8003950	$ 28.00	$ 24.92
SAP	SAP Workforce Performance Builder, Cloud	8003509-1	$ 109.00	$ 97.01
SAP	SAP Workforce Performance Builder, Cloud	8003509-2	$ 76.00	$ 67.64
SAP	SAP Workforce Performance Builder, Cloud	8003509-3	$ 64.00	$ 56.96
SAP	SAP Workforce Performance Builder, Cloud	8003509-4	$ 52.00	$ 46.28
SAP	SAP Workforce Performance Builder, Cloud	8003509-5	$ 43.00	$ 38.27
SAP	SAP Workforce Performance Builder, Cloud	8003509-6	$ 35.00	$ 31.15
SAP	SAP Workforce Performance Builder, Cloud	8003509-7	$ 29.00	$ 25.81
SAP	SAP Anywhere, starter bundle	8004078	$ 549.00	$ 488.61
SAP	SAP Anywhere, plus bundle	8004079	$ 934.00	$ 831.26
SAP	SAP Anywhere, premium bundle	8004080	$ 1,869.00	$ 1,663.41
SAP	SAP Anywhere, incremental user	8004084	$ 54.00	$ 48.06
SAP	SAP Anywhere, incremental channel	8004085	$ 109.00	$ 97.01
SAP	SAP HANA AppServices Compute Unit - Pro	8000348	$ 142.00	$ 126.38
SAP	SAP HANA AppServices Compute Unit - Prem	8000349	$ 208.00	$ 185.12
SAP	SAP HANA AppServices, Unstructured Storage	8000571	$ 11.00	$ 9.79
SAP	SAP HANA AppServices, Bandwidth	8000351	$ 4.40	$ 3.92
SAP	SAP HANA AppServices, 3rd Party Connect	8000573	$ 110.00	$ 97.90
SAP	SAP HANA AppServices, Administrator	8004159	$ 39.00	$ 34.71
SAP	SAP HANA AppServices, Cloud Portal	8004158	$ 193.00	$ 171.77
SAP	SAP HCP Starter Edition 32 GB	8001020	$ 439.00	$ 390.71
SAP	SAP HCP Starter Edition 64 GB	8001021	$ 549.00	$ 488.61
SAP	SAP HANA AppServices Custom Domains	8001022	$ 110.00	$ 97.90
SAP	SAP HANA Infrastructure Services 64 GB	8003366	$ 952.00	$ 847.28
SAP	SAP HANA Infrastructure Services 128 GB	8003367	$ 1,472.00	$ 1,310.08
SAP	SAP HANA Infrastructure Services 256 GB	8003368	$ 2,338.00	$ 2,080.82
SAP	SAP HANA Infrastructure Services 512 GB	8003369	$ 4,503.00	$ 4,007.67
SAP	SAP HANA Infrastructure Services 1024 GB	8003370	$ 6,668.00	$ 5,934.52
SAP	SAP HANA DBServices, base edition 32 GB	8003545	$ 1,375.00	$ 1,223.75
SAP	SAP HANA DBServices, base edition 64 GB	8003371	$ 2,602.00	$ 2,315.78
SAP	SAP HANA DBServices, base edition 128 GB	8003372	$ 4,772.00	$ 4,247.08
SAP	SAP HANA DBServices, base edition 256 GB	8003374	$ 8,938.00	$ 7,954.82
SAP	SAP HANA DBServices, base edition 512 GB	8003375	$ 17,703.00	$ 15,755.67
SAP	SAP HANA DBServices, base edition 1024 GB	8003376	$ 31,418.00	$ 27,962.02
SAP	SAP HANA DBServices, non-prod. base ed. 32 GB	8003547	$ 1,375.00	$ 1,223.75
SAP	SAP HANA DBServices, non-prod. base ed. 64 GB	8003377	$ 2,602.00	$ 2,315.78
SAP	SAP HANA DBServices, non-prod. base ed. 128 GB	8003378	$ 4,772.00	$ 4,247.08
SAP	SAP HANA DBServices, non-prod. base ed. 256 GB	8003379	$ 8,938.00	$ 7,954.82
SAP	SAP HANA DBServices, non-prod. base ed. 512 GB	8003380	$ 17,703.00	$ 15,755.67
SAP	SAP HANA DBServices, non-prod. base ed. 1024 GB	8003381	$ 31,418.00	$ 27,962.02
SAP	SAP HANA DBServices, platform edition 32 GB	8003546	$ 3,300.00	$ 2,937.00
SAP	SAP HANA DBServices, platform edition 64 GB	8003382	$ 6,232.00	$ 5,546.48
SAP	SAP HANA DBServices, platform edition 128 GB	8003383	$ 12,032.00	$ 10,708.48

SAP	SAP HANA DBServices, platform edition 256 GB	8003384	$ 23,458.00	$ 20,877.62
SAP	SAP HANA DBServices, platform edition 512 GB	8003385	$ 46,743.00	$ 41,601.27
SAP	SAP HANA DBServices, platform edition 1024 GB	8003386	$ 85,868.00	$ 76,422.52
SAP	SAP HANA DBServices, non-prod platform ed 32 GB	8003548	$ 3,300.00	$ 2,937.00
SAP	SAP HANA DBServices, non-prod platform ed 64 GB	8003387	$ 6,232.00	$ 5,546.48
SAP	SAP HANA DBServices, non-prod platform ed 128 GB	8003388	$ 12,032.00	$ 10,708.48
SAP	SAP HANA DBServices, non-prod. platform ed. 256 GB	8003389	$ 23,458.00	$ 20,877.62
SAP	SAP HANA DBServices, non-prod platform ed 512 GB	8003390	$ 46,743.00	$ 41,601.27
SAP	SAP HANA DBServices, non-prod platform ed 1024 GB	8003391	$ 85,868.00	$ 76,422.52
SAP	SAP HANA DBServices, ASE x-small	8003540	$ 550.00	$ 489.50
SAP	SAP HANA DBServices, ASE small	8003541	$ 770.00	$ 685.30
SAP	SAP HANA DBServices, ASE medium	8003542	$ 1,100.00	$ 979.00
SAP	SAP HANA DBServices, ASE large	8003543	$ 2,090.00	$ 1,860.10
SAP	SAP HANA DBServices, ASE x-large	8003544	$ 3,850.00	$ 3,426.50
SAP	SAP HANA DBServices, ASE non-production x-small	8003535	$ 550.00	$ 489.50
SAP	SAP HANA DBServices, ASE non-production small	8003536	$ 770.00	$ 685.30
SAP	SAP HANA DBServices, ASE non-production medium	8003537	$ 1,100.00	$ 979.00
SAP	SAP HANA DBServices, ASE non-production large	8003538	$ 2,090.00	$ 1,860.10
SAP	SAP HANA DBServices, ASE non-production x-large	8003539	$ 3,850.00	$ 3,426.50
SAP	SAP HANA Cloud Platform, professional edition	8003513	$ 22.00	$ 19.58
SAP	SAP HANA Cloud Platform, single application edition	8003514	$ 43.00	$ 38.27
SAP	SAP HANA Cloud Platform, multiple application edition	8003515	$ 130.00	$ 115.70
SAP	SAP HANA Cloud Platform gamification service	8004046	$ 1,100.00	$ 979.00
SAP	SAP HANA AppServices, standard edition	8003516	$ 1,089.00	$ 969.21
SAP	SAP HANA AppServices, premium edition	8003517	$ 3,619.00	$ 3,220.91
SAP	HANA Cloud Integration - Application Ed	8000800	$ 0.08	$ 0.08
SAP	HANA Cloud Integration Standard Edition	8002949	$ 2,200.00	$ 1,958.00
SAP	HANA Cloud Integration Professional Edition	8002951	$ 5,500.00	$ 4,895.00
SAP	HANA Cloud Integration, add'l connection	8002952	$ 385.00	$ 342.65
SAP	SAP HANA AppServices, Cloud Identity	8003511	$ 5.50	$ 4.90
SAP	SAP HANA AppServices, Web IDE Edition	8003103	$ 54.00	$ 48.06
SAP	SAP HCP, Remote Data Sync Service, standard edition	8003943	$ 587.00	$ 522.43
SAP	SAP HCP, Remote Data Sync Service, premium edition	8003944	$ 1,099.00	$ 978.11
SAP	SAP HCP Internet of Things Services	8003929	$ 2.20	$ 1.96
SAP	SAP TwoGo Location	8000776	$ 11.00	$ 9.79
SAP	SAP Mobile Documents Cloud, User	8000761	$ 4.40	$ 3.92
SAP	SAP Mobile Docs Cloud, Storage	8003298	$ 2.20	$ 1.96
SAP	SAP Mobile Secure, cloud edition	8004160	$ 1.65	$ 1.47
SAP	SAP Mobile App Protection by Mocana, cloud	8004161	$ 2.20	$ 1.96
SAP	SAP HCP Mobile Services, user	8003145	$ 5.50	$ 4.90
SAP	SAP HCP Mobile Services, consumer edition	8004024	$ 8,250.00	$ 7,342.50
SAP	SAP Forms as a Service	8003528	$ 4,400.00	$ 3,916.00
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-1	$ 147.00	$ 130.83
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-2	$ 246.00	$ 218.94
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-3	$ 494.00	$ 439.66
SAP	SAP Lumira Cloud, Enterprise Ed, User	8000783	$ 24.00	$ 21.36
SAP	SAP Lumira Cloud,Ent Ed,Storage (per GB)	8000784	$ 24.00	$ 21.36
SAP	SAP Cloud for Analytics, Analytics Std User Public Ed.	8004104	$ 127.00	$ 113.03
SAP	SAP Cloud for Analytics, Planning Prof User Public Ed.	8004105	$ 1,733.00	$ 1,542.37

SAP	SAP Cloud for Analytics, Planning Std User Public Ed.	8004106	$ 121.00	$ 107.69
SAP	SAP Cloud for Analytics, BI User Public Ed.	8004107	$ 22.00	$ 19.58
SAP	SAP Digital Boardroom, Public Ed.	8004108	$ 11,000.00	$ 9,790.00
SAP	SAP Cloud for Analytics, Analytics Std User Private Ed.	8004099	$ 198.00	$ 176.22
SAP	SAP Cloud for Analytics, Planning Prof User Private Ed.	8004100	$ 2,200.00	$ 1,958.00
SAP	SAP Cloud for Analytics, Planning Std User Private Ed.	8004101	$ 165.00	$ 146.85
SAP	SAP Cloud for Analytics, BI User Private Ed.	8004102	$ 66.00	$ 58.74
SAP	SAP Digital Boardroom, Private Ed.	8004103	$ 16,500.00	$ 14,685.00
SAP	SAP Cloud for Analytics, BI Extension Public Ed.	8004110	$ 22.00	$ 19.58
SAP	SAP Cloud for Analytics, storage add-on (per 10 GB)	8003359	$ 11.00	$ 9.79
SAP	SAP Cloud for Analytics test tenant 32 GB Private Ed.	8003351	$ 2,567.00	$ 2,284.63
SAP	SAP Cloud for Analytics test tenant 64 GB Private Ed.	8003352	$ 2,842.00	$ 2,529.38
SAP	SAP Cloud for Analytics test tenant 128 GB Private Ed.	8003353	$ 3,392.00	$ 3,018.88
SAP	SAP Cloud for Analytics test tenant 256 GB Private Ed.	8003354	$ 6,783.00	$ 6,036.87
SAP	SAP Cloud for Analytics 64 GB HANA upgrade, Private Ed.	8003614	$ 642.00	$ 571.38
SAP	SAP Cloud for Analytics 128 GB HANA upgrade, Private Ed.	8003355	$ 642.00	$ 571.38
SAP	SAP Cloud for Analytics 256 GB HANA upgrade, Private Ed.	8003356	$ 1,100.00	$ 979.00
SAP	SAP Cloud for Analytics 512 GB HANA upgrade, Private Ed.	8003357	$ 2,200.00	$ 1,958.00
SAP	SAP Cloud for Analytics 1024 GB HANA upgrade, Private Ed.	8003358	$ 2,750.00	$ 2,447.50
SAP	SAP Agile Data Preparation, cloud edition, technology foundation	8004122	$ 35,200.00	$ 31,328.00
SAP	SAP Agile Data Preparation, cloud edition, analyst option	8004123	$ 550.00	$ 489.50
SAP	SAP API Mgmt, standard cloud edition	8003674	$ 8,250.00	$ 7,342.50
SAP	SAP API Mgmt, premier cloud edition	8003676	$ 11,000.00	$ 9,790.00
SAP	SAP API Mgmt, enterprise cloud edition	8003677	$ 16,500.00	$ 14,685.00
SAP	Preferred Care, SuccessFactors	8003322	$ 0.20	
SAP	Preferred Care, SAP	8003430	$ 0.20	
SAP	Expert Care, Ariba	8002441	$ 0.30	
ServiceNow	ServiceNow® Additional Non-Production Instance - US Data Center (Monthly)	VOPADDINSTDC-US	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Additional Production Environment - US Data Center (Monthly)	ADDPRODENVRNMTUS	$ 3,750.00	$ 3,721.66
ServiceNow	ServiceNow® Approver User (Monthly)	SNCAPPROVER-36	$ 25.00	$ 24.81
ServiceNow	ServiceNow® Cloud Management - Node (250 Node Minimum Quantity)	SNCPROD90874	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Customer Service Management - Fulfiller User (Monthly)	SNCPROD103484	$ 125.00	$ 124.06
ServiceNow	ServiceNow® Discovery - Node (250 Node Minimum Quantity)	SNCPROD90840	$ 6.00	$ 5.95
ServiceNow	ServiceNow® Event Management - Node (250 Node Minimum Quantity)	SNCPROD90854	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Express Discovery (100 Pack) - Devices (Monthly)	SNCPROD01057	$ 20.00	$ 19.85
ServiceNow	ServiceNow® Express Discovery (1000 Pack - 500 Included at No Charge) - Devices (Monthly)	SNCPROD01056	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Express Fulfiller User (Monthly)	SNCEXPRESS	$ 50.00	$ 49.62
ServiceNow	ServiceNow® Facilities Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNFACILITIESSVC	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Financial Management - Fulfiller User (Monthly)	SNCFINMGMT	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Governance, Risk and Compliance Suite - Fulfiller User	SNCPROD90746	$ 125.00	$ 124.06
ServiceNow	ServiceNow® IT Financial Management - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCFINMGMTUN	$ 1.00	$ 0.99
ServiceNow	ServiceNow® IT Service Automation Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSVCSAUTSTEGVT-UR	$ 10.00	$ 9.92
ServiceNow	ServiceNow® ITSA Unlimited - Fulfiller User (Monthly)	SNITSAUNLTD	$ 350.00	$ 347.36
ServiceNow	ServiceNow® ITSA Unlimited (Including Platform Runtime) - Fulfiller User	SNCPROD90795	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Notify (All users) - User (Monthly)	SNCNOTIFYAL	$ 1.25	$ 1.24
ServiceNow	ServiceNow® Orchestration Client Software Distribution Application - Client Node (250 Node Minimum Quantity)	SNCPROD90836	$ 1.00	$ 0.99
ServiceNow	ServiceNow® Orchestration Core (10,000 Password Users and 1000 Client SW Dist. Client Nodes included) - Node (250 Node Minimum Quantity)	SNCPROD90863	$ 6.00	$ 5.95
ServiceNow	ServiceNow® Orchestration Password Reset Application - User (Monthly)	SNCORCHPASSWORD	$ 0.50	$ 0.50
ServiceNow	ServiceNow® Performance Analytics - Application (per $1000 Subscription) (Monthly)	SNCPERFANAUSER	$ 200.00	$ 198.49

ServiceNow	ServiceNow® Performance Analytics For IT Service Automation Suite - Application (per $1000 Subscription) (Monthly)	SNCPERFANAITSA	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Performance Analytics For Service Management Suite - Application (per $1000 Subscription) (Monthly)	SNCPERFANASERVMGMT	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Performance Analytics For Service Management Suite With Platform Runtime - Application (per $1000 Subscription) (Monthly)	SNCPROD90797	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Platform Runtime - Fulfiller User	SNCPROD90781	$ 35.00	$ 34.74
ServiceNow	ServiceNow® Project Portfolio Suite - Fulfiller User (Monthly)	SNCPROJPORTUF	$ 75.00	$ 74.43
ServiceNow	ServiceNow® Project Portfolio Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCPROJPORTU-UR	$ 8.00	$ 7.94
ServiceNow	ServiceNow® Public Catalog - Requests (Additonal Requests) (Monthly)	SNCPUBCATADD-36	$ 0.42	$ 0.42
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 1) (Monthly)	SNCPUBCAT1-36	$ 8,333.33	$ 8,270.36
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 2) (Monthly)	SNCPUBCAT2-36	$ 10,416.67	$ 10,337.95
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 3) (Monthly)	SNCPUBCAT3-36	$ 12,500.00	$ 12,405.54
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 4) (Monthly)	SNCPUBCAT4-36	$ 16,666.67	$ 16,540.72
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 5) (Monthly)	SNCPUBCAT5-36	$ 20,833.33	$ 20,675.90
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 2 (Up to 19999 Requests) (Monthly)	SNCPUBCAT1-2	$ 2,083.34	$ 2,067.60
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 3 (Up to 99999 Requests) (Monthly)	SNCPUBCAT1-3	$ 4,166.67	$ 4,135.18
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT1-4	$ 8,333.34	$ 8,270.37
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT1-5	$ 12,500.00	$ 12,405.54
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 3 (Up to 99999 Requests) (Monthly)	SNCPUBCAT2-3	$ 2,083.33	$ 2,067.59
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT2-4	$ 6,250.00	$ 6,202.77
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT2-5	$ 10,416.66	$ 10,337.94
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 3 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT3-4	$ 4,166.67	$ 4,135.18
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 3 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT3-5	$ 8,333.33	$ 8,270.36
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 4 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT4-5	$ 4,166.66	$ 4,135.17
ServiceNow	ServiceNow® Security Operations - Devices (250 Device Minimum Quantity) (Monthly)	SNCPROD104598	$ 0.75	$ 0.74
ServiceNow	ServiceNow® Security Operations (1,000 Devices Included) - Module (Monthly)	SNCPROD104565	$ 6,250.00	$ 6,202.77
ServiceNow	ServiceNow® Service Automation Platform Suite - Process User (Monthly)	SNCSVCSAUTPLT	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Catalog With Request Management - Unrestricted Users (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSERVCATREQMG	$ 3.00	$ 2.98
ServiceNow	ServiceNow® Service Management Suite - Fulfiller User (Monthly)	SNCSERVMGMT	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Management Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSERVMGMTUN	$ 20.00	$ 19.85
ServiceNow	ServiceNow® Service Management Suite With Platform Runtime - Fulfiller User	SNCPROD90798	$ 125.00	$ 124.06
ServiceNow	ServiceNow® ServiceWatch (Eureka and Fuji Only) - Nodes (250 Node Minimum Quantity) (Monthly)	SNCPROD125784	$ 17.00	$ 16.87
ServiceNow	ServiceNow® ServiceWatch Insight (Discovery, Service Mapping and Event Management included) - Node (250 Node Minimum Quantity)	SNCPROD90862	$ 17.00	$ 16.87
ServiceNow	ServiceNow® ServiceWatch Mapping (Discovery and Service Mapping included) - Node (250 Node Minimum Quantity)	SNCPROD90845	$ 14.00	$ 13.89
ServiceNow	ServiceNow® ServiceWatch Suite - Node (250 Node Minimum Quantity)	SNCPROD90911	$ 26.00	$ 25.80
ServiceNow	ServiceNow® Time Card User - Time Card User (Monthly)	SNCTIMECARD	$ 15.00	$ 14.89
ServiceNow	ServiceNow® Field Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNFIELDSVCAUTU	$ 7.00	$ 6.95
ServiceNow	ServiceNow® HR Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNCHRSERVICEU	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Edge Encryption - Application (per $1000 Subscription) User (Monthly)	SNCPROD01054	$ 200.00	$ 198.49
ServiceNow	ServiceNow® HR Service Management - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNCHRSERVICE	$ 5.00	$ 4.96
ServiceNow	ServiceNow® Service Management Suite v2 - Fulfiller User	SNCSERVMGMTV2	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Management Suite v2 With Platform Runtime - Fulfiller User	SNCSERVPLATRTV2	$ 125.00	$ 124.06
ServiceNow	ServiceNow® Service Strategy - Worker	SNCSERVSTRAT	$ 30.00	$ 29.77
ServiceNow	ServiceNow® Service Strategy - Planner	SNCSERVSTRAT	$ 75.00	$ 74.43
ServiceNow	ServiceNow® Service Strategy - Analyst	SNCSERVSTRAT	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - Public (per attendee)	PROD00975	$ 1,595.00	$ 1,582.95
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - On-Site Class (per attendee, minimum 5 attendees)	PROD00981	$ 1,595.00	$ 1,582.95
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - On-Site Class (additional attendee)	PROD00982	$ 1,595.00	$ 1,582.95
Virtru	VTRUEMAIL001	Virtru email encryption licen	$ 60.00	$ 58.65
Virtru	VTRUDRIVE002	Virtru Google Drive encryptic	$ 60.00	$ 58.65
Virtru	VTRUHIPAA003	Preconfigured DLP rules that	$ 499.00	$ 487.77

Virtru	VTRUTEMP004	Customer's logo added to the	$ 499.00	$ 487.77
Virtru	VTRUGTWY005	Server-side gateway that sca	$ 30,000.00	$ 29,325.00
Virtru	VTRUSR006	Customer's branding added t	$ 9,999.00	$ 9,774.02
Virtru	VTRUCLI007	Command line interace (CLI)	$ 1,999.00	$ 1,954.02
Virtustream	System Backup Setup	IC-DP-BU-1T	$ 500.00	$ 465.00
Virtustream	vHANA Installation and Setup Charge - Virtual Appliance	HM-HA-VIR-1T	$ 1,000.00	$ 930.00
Virtustream	Policy Auditor Service Setup	CS-VS-PSVC-1T	$ 62.50	$ 58.13
Virtustream	Policy Auditor System Setup	CS-VS-PSYS-1T	$ 1,500.00	$ 1,395.00
Virtustream	1 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-1TB	$ 6,924.60	$ 6,439.88
Virtustream	1 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-1TB	$ 6,924.60	$ 6,439.88
Virtustream	1 TB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-1TB	$ 7,883.96	$ 7,332.08
Virtustream	1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-1TB	$ 7,883.96	$ 7,332.08
Virtustream	1 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-1TB	$ 7,049.50	$ 6,556.03
Virtustream	1 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-1TB	$ 7,049.50	$ 6,556.03
Virtustream	1.5 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-15	$ 7,889.70	$ 7,337.43
Virtustream	1.5 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-15	$ 7,889.70	$ 7,337.43
Virtustream	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-2TB	$ 16,353.69	$ 15,208.93
Virtustream	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-2TB	$ 16,353.69	$ 15,208.93
Virtustream	2 TB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-2TB	$ 15,978.11	$ 14,859.65
Virtustream	2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-2TB	$ 15,978.11	$ 14,859.65
Virtustream	2 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-2TB	$ 8,438.34	$ 7,847.65
Virtustream	2 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-2TB	$ 8,438.34	$ 7,847.65
Virtustream	2FA Dedicated Base Fee	CS-2F-D1-SYS	$ 150.00	$ 139.50
Virtustream	2FA Dedicated DR Base Fee	CS-2F-D2-SYS	$ 45.00	$ 41.85
Virtustream	2FA Dedicated Token Fee	CS-2F-DT-MF	$ 9.00	$ 8.37
Virtustream	2FA Shared Token Fee	CS-2F-ST-MF	$ 11.00	$ 10.23
Virtustream	2FA Virtustream Portal Token Fee	CS-2F-VPT-MF	$ 9.00	$ 8.37
Virtustream	3 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-3TB	$ 9,613.54	$ 8,940.59
Virtustream	3 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-3TB	$ 9,613.54	$ 8,940.59
Virtustream	512 GB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-512	$ 5,472.60	$ 5,089.52
Virtustream	512 GB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-512	$ 5,472.60	$ 5,089.52
Virtustream	512 GB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-512	$ 6,533.21	$ 6,075.89
Virtustream	512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-512	$ 6,533.21	$ 6,075.89
Virtustream	6 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-6TB	$ 25,124.52	$ 23,365.81
Virtustream	6 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-6TB	$ 25,124.52	$ 23,365.81
Virtustream	Encryption Non-Production Agent per vCPU Fee	CS-ENC-AGTC-NP	$ 30.00	$ 27.90
Virtustream	Encryption Production Agent per vCPU Fee	CS-ENC-AGTC-PR	$ 60.00	$ 55.80
Virtustream	HANA Encryption Agent Fee (Non-Production)	CS-ENC-AGTH-NP	$ 125.00	$ 116.25
Virtustream	HANA Encryption Agent Fee (Production)	CS-ENC-AGTH-PR	$ 250.00	$ 232.50
Virtustream	Enterprise Basic Plus µVM	IC-UVM-BASP-ENT	$ 66.00	$ 61.38
Virtustream	Enterprise Reserve µVM	IC-UVM-RESV-ENT	$ 10.00	$ 9.30
Virtustream	Encryption Management System Fee	CS-ENC-SYS-SYS	$ 850.00	$ 790.50
Virtustream	Firewall Audit System	CS-FA-FA-SYS	$ 675.00	$ 627.75
Virtustream	Managed Firewall Auditing Service	CS-FA-MFA-SVC	$ 270.00	$ 251.10
Virtustream	Anti-Virus Primary System	CS-TM-AV1-SYS	$ 25.00	$ 23.25
Virtustream	Anti-Virus Secondary System	CS-TM-AV2-SYS	$ 25.00	$ 23.25
Virtustream	Anti-Virus Managed Service	CS-TM-AV-SVC	$ 24.99	$ 23.24
Virtustream	File Integrity Monitoring Primary System	CS-TM-FIM1-SYS	$ 25.00	$ 23.25
Virtustream	File Integrity Monitoring Secondary System	CS-TM-FIM2-SYS	$ 25.00	$ 23.25

Virtustream	High Memory Enterprise Basic Plus µVM	IC-UHV-BASP-ENT	$ 24.00	$ 22.32
Virtustream	High Memory Enterprise Basic Plus VM Fee	IC-HVM-BASP-ENT	$ 1,275.00	$ 1,185.75
Virtustream	High Memory Enterprise Reserve µVM	IC-UHV-RESV-ENT	$ 6.50	$ 6.05
Virtustream	Intrusion Detection and Firewall Primary System	CS-TM-IDFW1-SYS	$ 203.57	$ 189.32
Virtustream	Intrusion Detection and Firewall Secondary System	CS-TM-IDFW2-SYS	$ 25.00	$ 23.25
Virtustream	IPSec VPN Bandwidth Fee - USDC1	CS-VPN-U1-NET	$ 31.25	$ 29.06
Virtustream	IPSec VPN Bandwidth Fee - USDC2	CS-VPN-U2-NET	$ 31.25	$ 29.06
Virtustream	IPSec VPN Tunnel Managed Service	CS-VPN-T-SVC	$ 50.00	$ 46.50
Virtustream	Load Balancing Bandwidth Fee (Additional to Network Bandwidth)	IC-NW-LBM-NET	$ 22.50	$ 20.93
Virtustream	Intrusion Detection and Firewall Managed Service	CS-TM-IDFW-SVC	$ 73.74	$ 68.57
Virtustream	VM-Level Security Bundle Primary System fee	CS-TM-VLSB1-SYS	$ 190.18	$ 176.87
Virtustream	Managed Load Balancer Services (Per Server)	IC-NW-LBM-LB	$ 100.00	$ 93.00
Virtustream	VM-Level Security Bundle Secondary System fee	CS-TM-VLSB2-SYS	$ 56.25	$ 52.31
Virtustream	Managed Perimeter Firewall	CS-FW-MPF-SVC	$ 25.00	$ 23.25
Virtustream	Microsoft OS	IC-SW-MSS-WIN	$ 50.00	$ 46.50
Virtustream	Microsoft SQL Enterprise (Per 2 cores)	IC-SW-MQL-ENT	$ 575.00	$ 534.75
Virtustream	Microsoft SQL Standard (Per 2 cores)	IC-SW-MQL-STD	$ 150.00	$ 139.50
Virtustream	Network Bandwidth Fee - USDC1	CS-NW-BWU1-NET	$ 28.75	$ 26.74
Virtustream	Network Bandwidth Fee - USDC2	CS-NW-BWU2-NET	$ 28.75	$ 26.74
Virtustream	Network Based Intrusion Detection System and Managed Service - Secondary	CS-IDS-NB2-SYS	$ 477.00	$ 443.61
Virtustream	Network Based Intrusion Detection System and Managed Service - Primary	CS-IDS-NB1-SYS	$ 957.00	$ 890.01
Virtustream	VM-Level Security Bundle Service Fee (<101 VMs)	CS-TM-VLSBA-SVC	$ 116.14	$ 108.01
Virtustream	VM-Level Security Bundle Service Fee (<1001 VMs)	CS-TM-VLSBB-SVC	$ 105.92	$ 98.50
Virtustream	Public IP Address (IPv4)	IC-NW-IPAD-V4	$ 25.00	$ 23.25
Virtustream	Public IP Address (IPv6)	IC-NW-IPAD-V6	$ 5.00	$ 4.65
Virtustream	Red Hat Enterprise Linux - Enterprise (Per OS)	IC-SW-RHL-ENT	$ 100.00	$ 93.00
Virtustream	Red Hat Enterprise Linux - Standard (Per OS)	IC-SW-RHL-STD	$ 50.00	$ 46.50
Virtustream	Remote Desktop Services (Per User)	IC-SW-RDS-IF	$ 7.50	$ 6.98
Virtustream	SUSE Linux Enterprise <=2 vCPU & <=2GB RAM	IC-SW-SLES-2C	$ 110.00	$ 102.30
Virtustream	SUSE Linux Enterprise <=4 vCPU & <=8GB RAM	IC-SW-SLES-4C	$ 150.00	$ 139.50
Virtustream	SUSE Linux Enterprise <=8 vCPU & >8GB RAM	IC-SW-SLES-8C	$ 250.00	$ 232.50
Virtustream	SUSE Linux Enterprise > 8 vCPU & >8GB RAM	IC-SW-SLES-VCPU	$ 32.00	$ 29.76
Virtustream	SUSE Linux Enterprise for Physical HANA	IC-SW-SLES-PH	$ 200.00	$ 186.00
Virtustream	SUSE Linux Enterprise for SAP <=2 vCPU & <=2GB RAM	IC-SW-SLES-S2C	$ 200.00	$ 186.00
Virtustream	SUSE Linux Enterprise for SAP <=4 vCPU & <=8GB RAM	IC-SW-SLES-S4C	$ 275.00	$ 255.75
Virtustream	SUSE Linux Enterprise for SAP >4 vCPU or >8GB RAM	IC-SW-SLES-SVM	$ 325.00	$ 302.25
Virtustream	SUSE Linux Enterprise for Virtual HANA	IC-SW-SLES-VH	$ 73.00	$ 67.89
Virtustream	STABDARD System Backup (PROTECTED)- Local Only	IC-DP-BUP-LOC	$ 0.30	$ 0.28
Virtustream	STANDARD System Backup (PROTECTED) - Replicated	IC-DP-BUP-REP	$ 0.40	$ 0.37
Virtustream	HANA System Backup (Protected Data) - Local Only	IC-DP-BUPH-LOC	$ 1.35	$ 1.26
Virtustream	HANA System Backup (Protected Data) - Replicated	IC-DP-BUPH-REP	$ 1.80	$ 1.67
Virtustream	Tier 0 Block Storage - Local Only	IC-STO-T0A-LOC	$ 0.99	$ 0.92
Virtustream	Tier 0 Block Storage - Replicated	IC-STO-T0A-REP	$ 2.23	$ 2.07
Virtustream	Tier I Block Storage - Local Only	IC-STO-T1A-LOC	$ 0.53	$ 0.49
Virtustream	Tier I Block Storage - Replicated	IC-STO-T1A-REP	$ 1.16	$ 1.07
Virtustream	Tier II Block Storage - Local Only	IC-STO-T2A-LOC	$ 0.37	$ 0.34
Virtustream	Tier II Block Storage - Replicated	IC-STO-T2A-REP	$ 0.84	$ 0.78
Virtustream	Tier III Block Storage - Local Only	IC-STO-T3A-LOC	$ 0.16	$ 0.15
Virtustream	Tier III Block Storage – Replicated	IC-STO-T3A-REP	$ 0.42	$ 0.39

Virtustream	VM-Level Security Bundle Service Fee (<10,001 VMs)	CS-TM-VLSBC-SVC	$ 99.00	$ 92.07
Virtustream	VM-Level Security Bundle Service Fee (10,000+ VMs)	CS-TM-VLSBD-SVC	$ 88.72	$ 82.51
Virtustream	Log Management System Fee	CS-VS-LM-SYS	$ 2,000.00	$ 1,860.00
Virtustream	Managed Log Management Service	CS-VS-MLM-SVC	$ 60.00	$ 55.80
Virtustream	Policy Auditor Service Fee	CS-VS-PA-SVC	$ 73.00	$ 67.89
Virtustream	Policy Auditor System Fee	CS-VS-PA-SYS	$ 125.00	$ 116.25
Virtustream	Vulnerability Scanning Managed Service - non Public IP	CS-VS-NPIP-SVC	$ 100.00	$ 93.00
Virtustream	Vulnerability Scanning Remedial Ad Hoc Scan	CS-VS-NPIP-AH	$ 450.00	$ 418.50
Virtustream	Vulnerability Scanning Managed Service - Public IP	CS-VS-PIP-SVC	$ 500.00	$ 465.00
Virtustream	Co-Innovation Roundtables - Ad Hoc (6 months)	CC-TAM-CIR-AH	$ 5,850.00	$ 5,440.50
Virtustream	Demand Management Meetings - Ad Hoc (3 months)	CC-TAM-DMM-AH	$ 3,217.50	$ 2,992.28
Virtustream	Executive Scorecards - Ad Hoc (3 months)	CC-TAM-ES-AH	$ 3,510.00	$ 3,264.30
Virtustream	IT Resource Forecast - Ad Hoc (3 months)	CC-TAM-ITRF-AH	$ 7,020.00	$ 6,528.60
Virtustream	Reporting and Business Review - Ad Hoc (1 month)	CC-TAM-RBR-AH	$ 4,638.75	$ 4,314.04
Virtustream	Resource and Performance - Ad Hoc (1 month)	CC-TAM-RP-AH	$ 4,203.75	$ 3,909.49
Virtustream	SLA Review - Ad Hoc (1 month)	CC-TAM-SLAR-AH	$ 1,755.00	$ 1,632.15
Virtustream	Weekly Status and Incident Reporting - Ad Hoc (1 month)	CC-TAM-WSIR-AH	$ 3,330.00	$ 3,096.90
Virtustream	Cloud Cover Setup	CC-SVC-ONCC-1T	$ 155.00	$ 144.15
Virtustream	Onshore SAP User, Security, and Change Management Process Setup	CC-SAP-ONUS-1T	$ 2,750.00	$ 2,557.50
Virtustream	Onshore Business Operating System & Database Support	CC-NS-ONDB-BUS	$ 550.00	$ 511.50
Virtustream	Onshore Business Operating System Support	CC-NS-ONOS-BUS	$ 312.50	$ 290.63
Virtustream	Onshore Business SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-BUS	$ 1,031.25	$ 959.06
Virtustream	Onshore Business SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-BUS	$ 2,625.00	$ 2,441.25
Virtustream	Onshore Enterprise Operating System & Database Support	CC-NS-ONDB-ENT	$ 675.00	$ 627.75
Virtustream	Onshore Enterprise Operating System Support	CC-NS-ONOS-ENT	$ 406.25	$ 377.81
Virtustream	Onshore Enterprise SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-ENT	$ 2,625.00	$ 2,441.25
Virtustream	Onshore Enterprise SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-ENT	$ 3,625.00	$ 3,371.25
Virtustream	Onshore Standard Operating System & Database Support	CC-NS-ONDB-STD	$ 168.75	$ 156.94
Virtustream	Onshore Standard Operating System Support	CC-NS-ONOS-STD	$ 93.75	$ 87.19
Virtustream	Onshore Standard SAP Technical Support (Non-Prod)	CC-SAP-ONNH-STD	$ 406.25	$ 377.81
Virtustream	Onshore Standard SAP Technical Support (Prod)	CC-SAP-ONPH-STD	$ 687.50	$ 639.38
Virtustream	Operational Integration - 1 Year	CC-TAM-OPIN-1Y	$ 1,950.00	$ 1,813.50
Virtustream	Reporting and Business Review - 1 Year	CC-TAM-RBR-1Y	$ 3,092.50	$ 2,876.03
Virtustream	Resource and Performance - 1 Year	CC-TAM-RP-1Y	$ 2,802.50	$ 2,606.33
Virtustream	SLA Review - 1 Year	CC-TAM-SLAR-1Y	$ 1,170.00	$ 1,088.10
Virtustream	Technical Account Management (TAM) - Gold	CC-TAM-TAM-GOLD	$ 12,000.00	$ 11,160.00
Virtustream	Technical Account Management (TAM) - Silver	CC-TAM-TAM-SILV	$ 6,000.00	$ 5,580.00
Virtustream	Technical Account Manager (TAM) - Platinum	CC-TAM-TAM-PLAT	$ 24,000.00	$ 22,320.00
Virtustream	Technical Account Management (TAM) - Per Instance	CC-TAM-TAM-INST	$ 400.00	$ 372.00
Virtustream	Weekly Status and Incident Reporting - 1 Year	CC-TAM-WSIR-1Y	$ 2,220.00	$ 2,064.60
Virtustream	Rack & Stack (Full Cab) - USDC2	DC-RKU2-RS-1T	$ 1,562.50	$ 1,453.13
Virtustream	Rack & Stack (Full Cab) - USDC1	DC-RKU1-RS-1T	$ 1,562.50	$ 1,453.13
Virtustream	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (1 Hour)	DC-SVC-REU-SAH1	$ 150.00	$ 139.50
Virtustream	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (15 Minutes)	DC-SVC-REU-SAHQ	$ 37.50	$ 34.88
Virtustream	Remote Eyes & Hands (US) - Gold Ad Hoc (1 Hour)	DC-SVC-REU-GAH1	$ 175.00	$ 162.75
Virtustream	Remote Eyes & Hands (US) - Gold Ad Hoc (15 Minutes)	DC-SVC-REU-GAHQ	$ 43.75	$ 40.69
Virtustream	Cloud Connect - HA (48 ports available) - Setup - USDC1	DC-NWU1-XCH-1T	$ 650.00	$ 604.50
Virtustream	Cloud Connect - HA (48 ports available) - Setup - USDC2	DC-NWU2-XCH-1T	$ 650.00	$ 604.50
Virtustream	Cloud Connect - Standard (24 Ports Available) - Setup - USDC1	DC-NWU1-XCS-1T	$ 450.00	$ 418.50

Virtustream	Cloud Connect - Standard (24 Ports Available) - Setup - USDC2	DC-NWU2-XCS-1T	$ 450.00	$ 418.50
Virtustream	Coax Cross Connect - USDC1 - Installation	DC-NWU1-XCCX-1T	$ 200.00	$ 186.00
Virtustream	Coax Cross Connect - USDC2 - Installation	DC-NWU2-XCCX-1T	$ 200.00	$ 186.00
Virtustream	Copper Cross Connect - USDC1 - Installation	DC-NWU1-XCC-1T	$ 250.00	$ 232.50
Virtustream	Copper Cross Connect - USDC2 - Installation	DC-NWU2-XCC-1T	$ 250.00	$ 232.50
Virtustream	Fiber Cross Connect - USDC1 - Installation	DC-NWU1-XCF-1T	$ 500.00	$ 465.00
Virtustream	Fiber Cross Connect - USDC2 - Installation	DC-NWU2-XCF-1T	$ 500.00	$ 465.00
Virtustream	20 A / 120 V Power Strip - USDC1	DC-PWU1-21S-1T	$ 1,125.00	$ 1,046.25
Virtustream	20 A / 120 V Power Strip - USDC2	DC-PWU2-21S-1T	$ 1,125.00	$ 1,046.25
Virtustream	20 A / 120 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-21R-1T	$ 3,020.84	$ 2,809.38
Virtustream	20 A / 120 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-21R-1T	$ 4,479.16	$ 4,165.62
Virtustream	20 A / 120 V Primary Power - USDC1 - Installation	DC-PWU1-21P-1T	$ 1,979.16	$ 1,840.62
Virtustream	20 A / 120 V Primary Power - USDC2 - Installation	DC-PWU2-21P-1T	$ 2,916.66	$ 2,712.49
Virtustream	20 A / 208 V Power Strip - USDC1	DC-PWU1-22S-1T	$ 1,375.00	$ 1,278.75
Virtustream	20 A / 208 V Power Strip - USDC2	DC-PWU2-22S-1T	$ 1,375.00	$ 1,278.75
Virtustream	20 A / 208 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-22R-1T	$ 3,125.00	$ 2,906.25
Virtustream	20 A / 208 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-22R-1T	$ 4,687.50	$ 4,359.38
Virtustream	20 A / 208 V Primary Power - USDC1 - Installation	DC-PWU1-22P-1T	$ 2,083.34	$ 1,937.51
Virtustream	20 A / 208 V Primary Power - USDC2 - Installation	DC-PWU2-22P-1T	$ 3,229.16	$ 3,003.12
Virtustream	30 A / 120 V Power Strip - USDC1	DC-PWU1-31S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 120 V Power Strip - USDC2	DC-PWU2-31S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 120 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-31R-1T	$ 4,583.34	$ 4,262.51
Virtustream	30 A / 120 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-31R-1T	$ 7,291.66	$ 6,781.24
Virtustream	30 A / 120 V Primary Power - USDC1 - Installation	DC-PWU1-31P-1T	$ 3,125.00	$ 2,906.25
Virtustream	30 A / 120 V Primary Power - USDC2 - Installation	DC-PWU2-31P-1T	$ 5,000.00	$ 4,650.00
Virtustream	30 A / 208 V Power Strip - USDC1	DC-PWU1-32S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 208 V Power Strip - USDC2	DC-PWU2-32S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 208 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-32R-1T	$ 4,583.34	$ 4,262.51
Virtustream	30 A / 208 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-32R-1T	$ 7,708.34	$ 7,168.76
Virtustream	30 A / 208 V Primary Power - USDC1 - Installation	DC-PWU1-32P-1T	$ 3,333.34	$ 3,100.01
Virtustream	30 A / 208 V Primary Power - USDC2 - Installation	DC-PWU2-32P-1T	$ 5,625.00	$ 5,231.25
Virtustream	Rack Installation - USDC1	DC-RKU1-RK-1T	$ 5,000.00	$ 4,650.00
Virtustream	Rack Installation - USDC2	DC-RKU2-RK-1T	$ 5,000.00	$ 4,650.00
Virtustream	20 A / 120 V Primary / Redundant Power - USDC1	DC-PWU1-21R-PF	$ 534.06	$ 496.68
Virtustream	20 A / 120 V Primary / Redundant Power - USDC2	DC-PWU2-21R-PF	$ 576.89	$ 536.51
Virtustream	20 A / 120 V Primary Power - USDC1	DC-PWU1-21P-PF	$ 418.43	$ 389.14
Virtustream	20 A / 120 V Primary Power - USDC2	DC-PWU2-21P-PF	$ 463.76	$ 431.30
Virtustream	20 A / 208 V Primary / Redundant Power - USDC1	DC-PWU1-22R-PF	$ 823.85	$ 766.18
Virtustream	20 A / 208 V Primary / Redundant Power - USDC2	DC-PWU2-22R-PF	$ 898.09	$ 835.22
Virtustream	20 A / 208 V Primary Power - USDC1	DC-PWU1-22P-PF	$ 684.96	$ 637.01
Virtustream	20 A / 208 V Primary Power - USDC2	DC-PWU2-22P-PF	$ 759.20	$ 706.06
Virtustream	30 A / 120 V Primary / Redundant Power - USDC1	DC-PWU1-31R-PF	$ 731.65	$ 680.43
Virtustream	30 A / 120 V Primary / Redundant Power - USDC2	DC-PWU2-31R-PF	$ 795.89	$ 740.18
Virtustream	30 A / 120 V Primary Power - USDC1	DC-PWU1-31P-PF	$ 627.63	$ 583.70
Virtustream	30 A / 120 V Primary Power - USDC2	DC-PWU2-31P-PF	$ 695.65	$ 646.95
Virtustream	30 A / 208 V Primary / Redundant Power - USDC1	DC-PWU1-32R-PF	$ 1,166.34	$ 1,084.70
Virtustream	30 A / 208 V Primary / Redundant Power - USDC2	DC-PWU2-32R-PF	$ 1,277.69	$ 1,188.25
Virtustream	30 A / 208 V Primary Power - USDC1	DC-PWU1-32P-PF	$ 1,027.45	$ 955.53
Virtustream	30 A / 208 V Primary Power - USDC2	DC-PWU2-32P-PF	$ 1,138.80	$ 1,059.08

Virtustream	Cloud Connect - HA (48 ports available)	DC-NWU3-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - HA (48 ports available) - USDC1	DC-NWU1-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - HA (48 ports available) - USDC2	DC-NWU2-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - Standard (24 ports available)	DC-NWU3-XCS-STD	$ 250.00	$ 232.50
Virtustream	Cloud Connect - Standard (24 ports available) - USDC1	DC-NWU1-XCS-STD	$ 250.00	$ 232.50
Virtustream	Cloud Connect - Standard (24 ports available) - USDC2	DC-NWU2-XCS-STD	$ 250.00	$ 232.50
Virtustream	Coax DS-3 Cross Connect - USDC1	DC-NWU1-XCCX-MF	$ 175.00	$ 162.75
Virtustream	Coax DS-3 Cross Connect - USDC2	DC-NWU2-XCCX-MF	$ 175.00	$ 162.75
Virtustream	Copper Cross Connect - USDC1	DC-NWU1-XCC-MF	$ 187.50	$ 174.38
Virtustream	Copper Cross Connect - USDC2	DC-NWU2-XCC-MF	$ 187.50	$ 174.38
Virtustream	Fiber Cross Connect - USDC1	DC-NWU1-XCF-MF	$ 343.75	$ 319.69
Virtustream	Fiber Cross Connect - USDC2	DC-NWU2-XCF-MF	$ 343.75	$ 319.69
Virtustream	Hotel Rack (1U) - Managed Colo - USDC1	DC-RKU1-RK-HR	$ 125.00	$ 116.25
Virtustream	Hotel Rack (1U) - Managed Colo - USDC2	DC-RKU2-RK-HR	$ 125.00	$ 116.25
Virtustream	kW Primary Power Charge - USDC1	DC-PWU1-P-PF	$ 217.93	$ 202.67
Virtustream	kW Primary Power Charge - USDC2	DC-PWU2-P-PF	$ 217.93	$ 202.67
Virtustream	Remote Eyes & Hands (US) - Bronze	DC-SVC-REU-B	$ 300.00	$ 279.00
Virtustream	Remote Eyes & Hands (US) - Gold	DC-SVC-REU-G	$ 1,500.00	$ 1,395.00
Virtustream	Co-Innovation Roundtables - Ad Hoc (6 months)	CC-TAM-CIR-AH	$ 5,850.00	$ 5,265.00
Virtustream	Demand Management Meetings - Ad Hoc (3 months)	CC-TAM-DMM-AH	$ 3,217.50	$ 2,895.75
Virtustream	Executive Scorecards - Ad Hoc (3 months)	CC-TAM-ES-AH	$ 3,510.00	$ 3,159.00
Virtustream	IT Resource Forecast - Ad Hoc (3 months)	CC-TAM-ITRF-AH	$ 7,020.00	$ 6,318.00
Virtustream	Reporting and Business Review - Ad Hoc (1 month)	CC-TAM-RBR-AH	$ 4,638.75	$ 4,174.88
Virtustream	Resource and Performance - Ad Hoc (1 month)	CC-TAM-RP-AH	$ 4,203.75	$ 3,783.38
Virtustream	SLA Review - Ad Hoc (1 month)	CC-TAM-SLAR-AH	$ 1,755.00	$ 1,579.50
Virtustream	Weekly Status and Incident Reporting - Ad Hoc (1 month)	CC-TAM-WSIR-AH	$ 3,330.00	$ 2,997.00
Virtustream	Cloud Cover Setup	CC-SVC-ONCC-1T	$ 155.00	$ 139.50
Virtustream	Onshore SAP User, Security, and Change Management Process Setup	CC-SAP-ONUS-1T	$ 2,750.00	$ 2,475.00
Virtustream	Onshore Business Operating System & Database Support	CC-NS-ONDB-BUS	$ 550.00	$ 495.00
Virtustream	Onshore Business Operating System Support	CC-NS-ONOS-BUS	$ 312.50	$ 281.25
Virtustream	Onshore Business SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-BUS	$ 1,031.25	$ 928.13
Virtustream	Onshore Business SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-BUS	$ 2,625.00	$ 2,362.50
Virtustream	Onshore Enterprise Operating System & Database Support	CC-NS-ONDB-ENT	$ 675.00	$ 607.50
Virtustream	Onshore Enterprise Operating System Support	CC-NS-ONOS-ENT	$ 406.25	$ 365.63
Virtustream	Onshore Enterprise SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-ENT	$ 2,625.00	$ 2,362.50
Virtustream	Onshore Enterprise SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-ENT	$ 3,625.00	$ 3,262.50
Virtustream	Onshore Standard Operating System & Database Support	CC-NS-ONDB-STD	$ 168.75	$ 151.88
Virtustream	Onshore Standard Operating System Support	CC-NS-ONOS-STD	$ 93.75	$ 84.38
Virtustream	Onshore Standard SAP Technical Support (Non-Prod)	CC-SAP-ONNH-STD	$ 406.25	$ 365.63
Virtustream	Onshore Standard SAP Technical Support (Prod)	CC-SAP-ONPH-STD	$ 687.50	$ 618.75
Virtustream	Operational Integration - 1 Year	CC-TAM-OPIN-1Y	$ 1,950.00	$ 1,755.00
Virtustream	Reporting and Business Review - 1 Year	CC-TAM-RBR-1Y	$ 3,092.50	$ 2,783.25
Virtustream	Resource and Performance - 1 Year	CC-TAM-RP-1Y	$ 2,802.50	$ 2,522.25
Virtustream	SLA Review - 1 Year	CC-TAM-SLAR-1Y	$ 1,170.00	$ 1,053.00
Virtustream	Technical Account Management (TAM) - Gold	CC-TAM-TAM-GOLD	$ 12,000.00	$ 10,800.00
Virtustream	Technical Account Management (TAM) - Silver	CC-TAM-TAM-SILV	$ 6,000.00	$ 5,400.00
Virtustream	Technical Account Manager (TAM) - Platinum	CC-TAM-TAM-PLAT	$ 24,000.00	$ 21,600.00
Virtustream	Technical Account Management (TAM) - Per Instance	CC-TAM-TAM-INST	$ 400.00	$ 360.00
Virtustream	Weekly Status and Incident Reporting - 1 Year	CC-TAM-WSIR-1Y	$ 2,220.00	$ 1,998.00

VMware	U.S. Federal Socialcast Configuration and Integration Design - On Premise Platform	CON-HZ-SC-CIDOP-FF	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal Socialcast Assigned Client Account Representative	CON-HZ-SC-ACAR-FF	$ 30,000.00	$ 29,319.90
VMware	U.S. Federal Socialcast Reach System Integration	CON-HZ-SC-RSI-FF	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal Socialcast Single Sign On Configuration	CON-HZ-SC-SSOC-FF	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal Socialcast Custom Theme Integration	CON-HZ-SC-CTI-FF	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Open Enrollment	EDU-SRMICM58-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Onsite	EDU-SRMICM58-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Extra Person	EDU-SRMICM58-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - Open Enrollment	EDU-VSDW55-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - On Site	EDU-VSDW55-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - Extra Person	EDU-VSDW55-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - Open Enrollment	EDU-SDDC3-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - On Site	EDU-SDDC3-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - Extra Person	EDU-SDDC3-XP-F	$ 5,285.00	$ 5,165.19
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - Open Enrollment	EDU-NSXFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - On Site	EDU-NSXFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - Extra Person	EDU-NSXFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	VMware Mirage: Install Configure Manage [V5.0] - Open Enrollment	EDU-MICM5-OE-F	$ 2,250.00	$ 2,198.99
VMware	VMware Mirage: Install Configure Manage [V5.0] - Onsite	EDU-MICM5-OS-F	$ 18,750.00	$ 18,324.94
VMware	VMware Mirage: Install Configure Manage [V5.0] - Extra Person	EDU-MICM5-XP-F	$ 1,875.00	$ 1,832.49
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V6.0] - Open Enrollment	EDU-VSOS6-OE-F	$ 4,475.00	$ 4,373.55
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V6.0] - On Site	EDU-VSOS6-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V6.0] - Open Enrollment	EDU-VSICM6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V6.0] - On Site	EDU-VSICM6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V 6.0] - Extra Person	EDU-VSICM6-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware vFabric tcServer Jumpstart	CON-S2-TCSERVER-JS-F	$ 5,495.00	$ 5,370.43
VMware	U.S. Federal VMware vFabric Hyperic Jumpstart	CON-S2-HYPERIC-JS-F	$ 8,195.00	$ 8,009.22
VMware	U.S. Federal VMware vFabric Hyperic and tcServer Jumpstart	CON-S2-HYPR-TCS-JS-F	$ 12,795.00	$ 12,504.94
VMware	U.S. Federal VMware vFabric PaaS Planning Service	CON-S2-PAAS-PLN-F	$ 25,595.00	$ 25,014.76
VMware	U.S. Federal GemFire Architectural Accelerator Service	CON-S2-GEMFIRE-ACL-F	$ 25,595.00	$ 25,014.76
VMware	U.S. Federal VMware Hyperic and vCenter Operations Enterprise Standalone Jumpstart	CON-S2-HYPR-VCO-JS-F	$ 18,995.00	$ 18,564.38
VMware	U.S. Federal VMware Advanced Technical Account Manager for NSX	TAM-NSX-ADV-F	$ 174,995.00	$ 171,027.86
VMware	U.S. Federal VMware Basic Technical Account Manager for NSX	TAM-NSX-BSC-F	$ 89,995.00	$ 87,954.81
VMware	U.S. Federal VMware Dedicated Technical Account Manager for NSX	TAM-NSX-DED-F	$ 324,995.00	$ 317,627.36
VMware	U.S. Federal VMware Infrastructure Health Check	CON-ESX-HC-AW-F	$ 9,000.00	$ 8,795.97
VMware	U.S. Federal VMware Physical to Virtual Migration Jumpstart	CON-ESX-P2V-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware Infrastructure with vCenter Lab Manager Jumpstart	CON-ESXVC-LM-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal VMware Infrastructure with Physical to Virtual Migration Jumpstart	CON-ESXVCP2V-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal VMware Infrastructure Jumpstart with vCenter Stage Manager	CON-ESXVCSM-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal Consulting Expense Reimbursement (T&E)	CON-EXP-F	$ 2,200.00	$ 2,150.13
VMware	U.S. Federal Vmware 1-day Jumpstart Add-on	CON-GC-JSAO-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware vCenter Lab Manager Jumpstart	CON-LM-JS-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware ThinApp Application Virtualization Jumpstart	CON-THIN-JS-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware View Manager Jumpstart	CON-VIEW-JS-F	$ 9,000.00	$ 8,795.97
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 1 to Tier 2 per Month	TAM-UG-TIER-1-2-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 1 to Tier 3 per Month	TAM-UG-TIER-1-3-F	$ 19,583.33	$ 19,139.38
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 2 to Tier 3 per Month	TAM-UG-TIER-2-3-F	$ 12,083.33	$ 11,809.40
VMware	U.S. Federal VMware View 4: Install Configure Manage - Open Enrollment	EDU-VMVICM-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware View 4: Install Configure Manage - Onsite	EDU-VMVICM-OS-F	$ 20,625.00	$ 20,157.43

VMware	U.S. Federal VMware View 4: Install Configure Manage - Extra Person	EDU-VMVICM-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - Extra Person	EDU-VS4DMP-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vSphere 4: Design Workshop - Open Enrollment	EDU-VS4DW-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware vSphere 4: Design Workshop - On Site	EDU-VS4DW-OS-F	$ 20,625.00	$ 20,157.43
VMware	U.S. Federal VMware vSphere 4: Design Workshop - Extra Person	EDU-VS4DW-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware vSphere 4: Manage Availability - Open Enrollment	EDU-VS4MA-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal VMware vSphere 4: Manage Availability - On Site	EDU-VS4MA-OS-F	$ 6,875.00	$ 6,719.14
VMware	U.S. Federal VMware vSphere 4: Manage Availability - Extra Person	EDU-VS4MA-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - Open Enrollment	EDU-VS4MDS-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - On Site	EDU-VS4MDS-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - Extra Person	EDU-VS4MDS-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - Open Enrollment	EDU-VS4MP-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - On Site	EDU-VS4MP-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - Open Enrollment	EDU-VS4MS-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - On Site	EDU-VS4MS-OS-F	$ 6,875.00	$ 6,719.14
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - Extra Person	EDU-VS4MS-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal VMware vSphere 4: Skills for Operators - Open Enrollment	EDU-VS4SO-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere 4: Skills for Operators - Onsite	EDU-VS4SO-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere 4: Skills for Operators- Extra Person	EDU-VS4SO-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - Open Enrollment	EDU-VS4TR-OE-F	$ 3,595.00	$ 3,513.50
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - On Site	EDU-VS4TR-OS-F	$ 30,200.00	$ 29,515.37
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - Extra Person	EDU-VS4TR-XP-F	$ 3,020.00	$ 2,951.54
VMware	U.S. Federal VMware vSphere 4: What's New - Open Enrollment	EDU-VS4WN-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere 4: What's New-On Site	EDU-VS4WN-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere 4: What's New-Extra Person	EDU-VS4WN-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal Vmware VS4: Install Configure Manage V40b - Extra Person	EDU-VS41ICM-XP-F	$ 3,438.00	$ 3,360.06
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Open Enrollment	EDU-VDFT45-OE-F	$ 4,945.00	$ 4,832.90
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Onsite	EDU-VDFT45-OS-F	$ 41,580.00	$ 40,637.38
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Extra Person	EDU-VDFT45-XP-F	$ 4,158.00	$ 4,063.74
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Open Enrollment	EDU-VS4AFT-OE-F	$ 5,600.00	$ 5,473.05
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Onsite	EDU-VS4AFT-OS-F	$ 47,190.00	$ 46,120.20
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Extra Person	EDU-VS4AFT-XP-F	$ 4,719.00	$ 4,612.02
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Open Enrollment	EDU-VS41AUFT-OE-F	$ 5,165.00	$ 5,047.91
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Onsite	EDU-VS41AUFT-OS-F	$ 43,450.00	$ 42,464.99
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Extra Person	EDU-VS41AUFT-XP-F	$ 4,345.00	$ 4,246.50
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V5.0] - On Site	EDU-VSICM5-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V5.0] - Extra Person	EDU-VSICM5-XP-F	$ 3,438.00	$ 3,360.06
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - Open Enrollment	EDU-VSWN5-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - On Site	EDU-VSWN5-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - Extra Person	EDU-VSWN5-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - Open Enrollment	EDU-VCSRM5-OE-F	$ 1,795.00	$ 1,754.31
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - On Site	EDU-VCSRM5-OS-F	$ 15,100.00	$ 14,757.68
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - Extra Person	EDU-VCSRM5-XP-F	$ 1,510.00	$ 1,475.77
VMware	U.S. Federal VMware vSphere: Fast Track [V5.0] - On Site	EDU-VSFT5-OS-F	$ 55,000.00	$ 53,753.15
VMware	U.S. Federal VMware vSphere: Fast Track [V5.0] - Extra Person	EDU-VSFT5-XP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - Open Enrollment	EDU-VC15DM-OE-F	$ 3,595.00	$ 3,513.50
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - On Site	EDU-VC15DM-OS-F	$ 30,200.00	$ 29,515.37
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - Extra Person	EDU-VC15DM-XP-F	$ 3,020.00	$ 2,951.54
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - Open Enrollment	EDU-VSOS5-OE-F	$ 4,495.00	$ 4,393.10

VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - On Site	EDU-VSOS5-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - Extra Person	EDU-VSOS5-XP-F	$ 3,775.00	$ 3,689.42
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - Open Enrollment	EDU-VCOAP5-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - On Site	EDU-VCOAP5-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - Extra Person	EDU-VCOAP5-XP-F	$ 1,375.00	$ 1,343.83
VMware	VMware View: Design Best Practices [V5.1] - Open Enrollment	EDU-VDBP51-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware View: Design Best Practices [V5.1] - On Site	EDU-VDBP51-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware View: Design Best Practices [V5.1] - Extra Person	EDU-VDBP51-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware View: Desktop Fast Track [V5.0] - On Site	EDU-VDFT5-OS-F	$ 37,818.00	$ 36,960.66
VMware	U.S. Federal VMware View: Desktop Fast Track [V5.0] - Extra Person	EDU-VDFT5-XP-F	$ 3,782.00	$ 3,696.26
VMware	VMware vCloud: Design Best Practices [V1.5] - Open Enrollment	EDU-VCDBP15-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware vCloud: Design Best Practices [V1.5] - On Site	EDU-VCDBP15-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware vCloud: Design Best Practices [V1.5] - Extra Person	EDU-VCDBP15-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vFabric TAM	CON-S2-TAM-TIER-1-F	$ 64,995.00	$ 63,521.56
VMware	U.S. Federal VMware vFabric Strategic TAM	CON-S2-TAM-TIER-2-F	$ 154,995.00	$ 151,481.26
VMware	U.S. Federal VMware vFabric Dedicated Strategic TAM	CON-S2-TAM-TIER-3-F	$ 299,995.00	$ 293,194.11
VMware	U.S. Federal Spring Web [V3.1] - Onsite	EDU-S2-PRIV-SW31-OS-F	$ 2,025.00	$ 2,025.00
VMware	Groovy and Grails [V2.0] - Open Enrollment	EDU-S2-GG20-OE-F	$ 2,700.00	$ 2,638.79
VMware	Groovy and Grails [V2.0] - Onsite	EDU-S2-PRIV-GG20-OS-F	$ 2,025.00	$ 1,979.09
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - Open Enrollment	EDU-VCNS51-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - On Site	EDU-VCNS51-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - Extra Person	EDU-VCNS51-XP-F	$ 2,265.00	$ 2,213.65
VMware	VMware vCloud Director: Organization Administration [V5.5] - Open Enrollment	EDU-VCOA55-OE-F	$ 1,645.00	$ 1,607.71
VMware	VMware vCloud Director: Organization Administration [V5.5] - On Site	EDU-VCOA55-OS-F	$ 13,750.00	$ 13,438.29
VMware	VMware vCloud Director: Organization Administration [V5.5] - Extra Person	EDU-VCOA55-XP-F	$ 1,375.00	$ 1,343.83
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - Open Enrollment	EDU-VCICM55-OE-F	$ 2,475.00	$ 2,418.89
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - On Site	EDU-VCICM55-OS-F	$ 20,625.00	$ 20,157.43
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - Extra Person	EDU-VCICM55-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - Open Enrollment	EDU-VICM5-OE-F	$ 3,295.00	$ 3,220.30
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - On Site	EDU-VICM5-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - Open Enrollment	EDU-VSWN6-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - On Site	EDU-VSWN6-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - Extra Person	EDU-VSWN6-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - Open Enrollment	EDU-M5H6FT-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - On Site	EDU-M5H6FT-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - Extra Person	EDU-M5H6FT-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - Open Enrollment	EDU-ITBM8-OE-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - On Site	EDU-ITBM8-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - Extra Person	EDU-ITBM8-XP-F	$ 2,752.00	$ 2,689.61
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - On Site	EDU-VCOPICM6-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - Open Enrollment	EDU-VCOPICM6-OE-F	$ 4,495.00	$ 4,393.10
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - Extra Person	EDU-VCOPICM6-XP-F	$ 3,775.00	$ 3,689.42
VMware	U.S. Federal VMware Horizon 6 Production Pilot	CON-HZN-PILOT-F	$ 74,380.00	$ 72,693.80
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - Open Enrollment	EDU-AW-BTCMP-OE-F	$ 2,800.00	$ 2,736.52
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - On Site	EDU-AW-BTCMP-OS-F	$ 16,800.00	$ 16,419.14
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - Extra Person	EDU-AW-BTCMP-XP-F	$ 2,240.00	$ 2,189.22
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - Open Enrollment	EDU-AW-INTEG-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - On Site	EDU-AW-INTEG-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - Extra Person	EDU-AW-INTEG-XP-F	$ 1,320.00	$ 1,290.08

VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - Open Enrollment	EDU-AW-K12-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - On Site	EDU-AW-K12-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - Extra Person*	EDU-AW-K12-XP-F	$ 1,320.00	$ 1,290.08
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - Open Enrollment	EDU-AW-MANAGE-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - On Site	EDU-AW-MANAGE-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - Extra Person	EDU-AW-MANAGE-XP-F	$ 1,320.00	$ 1,290.08
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutions - Open Enrollment	EDU-AW-ONPREM-OE-F	$ 895.00	$ 874.71
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutions - On Site Dedicated	EDU-AW-ONPREM-OS-F	$ 5,370.00	$ 5,248.26
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutionsy - Extra Person	EDU-AW-ONPREM-XP-F	$ 716.00	$ 699.77
VMware	U.S. Federal VMware vSphere: Bootcamp [V6] - Open Enrollment	EDU-BOOT6-OE-F	$ 7,145.00	$ 6,983.02
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - Open Enrollment	EDU-HDD6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - On Site	EDU-HDD6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - Extra Person	EDU-HDD6-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - Open Enrollment	EDU-HICM62-OE-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - On Site	EDU-HICM62-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - Extra Person	EDU-HICM62-XP-F	$ 2,752.00	$ 2,689.61
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - Open Enrollment	EDU-NSXFT61-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - On Site	EDU-NSXFT61-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - Extra Person	EDU-NSXFT61-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - Open Enrollment	EDU-NSXICM62-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - On Site	EDU-NSXICM62-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - Extra Person	EDU-NSXICM62-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware Site Recovery Manager: Install Configure Manage [V6.1] - Open Enrollment	EDU-SRMICM61-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. FederalVMware Site Recovery Manager: Install Configure Manage [V6.1] - On Site	EDU-SRMICM61-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware Site Recovery Manager: Install Configure Manage [V6.1] - Extra Person	EDU-SRMICM61-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - Open Enrollment	EDU-VCADDFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - On Site	EDU-VCADDFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - Extra Person	EDU-VCADDFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - On Premise (Includes Production Sup	EDU-VOSTFT6-OE-F	$ 6,265.00	$ 5,996.73
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Producti	EDU-VOSTFT6-OS-F	$ 52,850.00	$ 50,586.90
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Produ	EDU-VOSTFT6-XP-F	$ 5,285.00	$ 5,058.69
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - Open Enrollment	EDU-VRAICM62-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - On Site	EDU-VRAICM62-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - Extra Person	EDU-VRAICM62-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - Open Enrollment	EDU-VRAICM7-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - On Site	EDU-VRAICM7-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - Extra Person	EDU-VRAICM7-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Product	EDU-VROPSOP60-OE-F	$ 1,650.00	$ 1,579.35
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - Open Enrollment	EDU-VSANDM6-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - On Site	EDU-VSANDM6-OS-F	$ 20,625.00	$ 20,157.43
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - Extra Person	EDU-VSANDM6-XP-F	$ 2,064.00	$ 2,017.21
VMware	U.S. Federal VMware vSphere Bootcamp - Onsite	EDU-VSBC-OS-F	$ 54,600.00	$ 53,362.22
VMware	U.S. Federal VMware vSphere Bootcamp - Extra Student	EDU-VSBC-XP-F	$ 5,460.00	$ 5,336.22
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - Open Enrollment	EDU-VSDDFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - On Site	EDU-VSDDFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - Extra Person	EDU-VSDDFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware vSphere: Skills for Operators - Open Enrollment	EDU-VSO6-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vSphere: Skills for Operators - On Site	EDU-VSO6-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: Skills for Operators - Extra Person	EDU-VSO6-XP-F	$ 1,376.00	$ 1,344.81

VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - Open Enrollment	EDU-VTSW6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - On Site	EDU-VTSW6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - Extra Person	EDU-VTSW6-XP-F	$ 755.00	$ 737.88
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-DLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-APP-DLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-DLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 1 year	V-APP-PLL-D-F	$ 25.00	$ 23.93
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 3 years	V-APP-SSS-D-3G-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-SSS-D-3P-F	$ 15.84	$ 15.16
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 1 year	V-APP-SSS-D-G-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 3 years	V-APP-SSS-D-P-F	$ 6.00	$ 5.74
VMware	TPP L3 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-2G-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Blue Management Suite On-Premise - Includes 3 days On-Site	V-BMS-CLD-D-2P-F	$ 151.00	$ 144.53
VMware	TPP L4 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-3G-F	$ 201.00	$ 192.39
VMware	U.S. Federal VMware AirWatch Blue Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-CLD-D-3P-F	$ 212.00	$ 202.92
VMware	TPP L2 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-G-F	$ 76.00	$ 72.75
VMware	TPP L5 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-P-F	$ 80.00	$ 76.57
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-2G-F	$ 286.00	$ 273.75
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-2P-F	$ 299.00	$ 286.20
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-3G-F	$ 402.00	$ 384.79
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-3P-F	$ 420.00	$ 402.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-G-F	$ 152.00	$ 145.49
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-P-F	$ 159.00	$ 152.19
VMware	U.S. Federal VMware AirWatch Green Management Suite On-Premise - Includes 2 days On-Site	V-BMS-DLD-D-2G-F	$ 166.00	$ 158.89
VMware	U.S. Federal VMware AirWatch Orange Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-DLD-D-2P-F	$ 173.00	$ 165.59
VMware	U.S. Federal VMware AirWatch Green Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-DLD-D-3G-F	$ 233.00	$ 223.02
VMware	U.S. Federal VMware AirWatch On-Premise Weekend Upgrades and Off-Hours Requiring Same Region One Time Fee	V-BMS-DLD-D-3P-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch End User On-Boarding Video	V-BMS-DLD-D-G-F	$ 88.00	$ 84.23
VMware	U.S. Federal VMware AirWatch Orange Management Suite On-Premise - Includes 2 days On-Site	V-BMS-DLD-D-P-F	$ 92.00	$ 88.06
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-DLD-U-2G-F	$ 331.00	$ 316.83
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-2P-F	$ 345.00	$ 330.23
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-3G-F	$ 465.00	$ 445.09
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-BMS-DLD-U-3P-F	$ 484.00	$ 463.27
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-DLD-U-G-F	$ 176.00	$ 168.46
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-P-F	$ 183.00	$ 175.16
VMware	U.S. Federal VMware AirWatch SaaS SEG and MAG Upgrade	V-BMS-OPL-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware AirWatch Yellow Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-OPL-D-2P-F	$ 128.00	$ 122.52
VMware	U.S. Federal VMware AirWatch SaaS SEG and MAG Weekend and Same Region Off-Hours Upgrade	V-BMS-OPL-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Green Management Suite Perpetual: 1 Device	V-BMS-OPL-D-3P-F	$ 180.00	$ 172.29
VMware	U.S. Federal VMware AirWatch SocialCast Dedicated SaaS Setup Fee One Time Fee	V-BMS-OPL-D-G-F	$ 64.00	$ 61.26

VMware	U.S. Federal VMware AirWatch Yellow Management Suite On-Premise - Includes 3 days On-Site	V-BMS-OPL-D-P-F	$ 68.00	$ 65.09
VMware	TPP L3 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-PLL-D-F	$ 90.00	$ 86.15
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 1 year	V-BMS-PLL-U-F	$ 180.00	$ 172.29
VMware	U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extension (25 (	V-BMS-SSS-D-3G-F	$ 50.16	$ 48.01
VMware	TPP L1 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-SSS-D-3P-F	$ 60.72	$ 58.12
VMware	TPP L4 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-SSS-D-G-F	$ 19.00	$ 18.19
VMware	TPP L5 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-SSS-D-P-F	$ 23.00	$ 22.02
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 3 years	V-BMS-SSS-U-3G-F	$ 100.32	$ 96.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-SSS-U-3P-F	$ 118.80	$ 113.71
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 1 year	V-BMS-SSS-U-G-F	$ 38.00	$ 36.37
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 3 years	V-BMS-SSS-U-P-F	$ 45.00	$ 43.07
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-2P-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-3P-F	$ 135.00	$ 129.22
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-P-F	$ 51.00	$ 48.82
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 Device for 1 year	V-CLC-DLD-D-2G-F	$ 115.00	$ 110.08
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 Device for 3 years	V-CLC-DLD-D-2P-F	$ 119.00	$ 113.90
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 Device for 1 year	V-CLC-DLD-D-3G-F	$ 162.00	$ 155.06
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-DLD-D-3P-F	$ 167.00	$ 159.85
VMware	U.S. Federal VMware AirWatch Video Perpetual: 1 Device	V-CLC-DLD-D-G-F	$ 61.00	$ 58.39
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 Device for 3 years	V-CLC-DLD-D-P-F	$ 63.00	$ 60.30
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 Device for 1 year	V-CLV-CLD-D-2G-F	$ 57.00	$ 54.56
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 Device for 3 years	V-CLV-CLD-D-2P-F	$ 59.00	$ 56.47
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 Device for 1 year	V-CLV-CLD-D-3G-F	$ 80.00	$ 76.57
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-CLD-D-3P-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware AirWatch Telecom Perpetual: 1 Device	V-CLV-CLD-D-G-F	$ 30.00	$ 28.72
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 Device for 3 years	V-CLV-CLD-D-P-F	$ 31.00	$ 29.67
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-2G-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-2P-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-3G-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-3P-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-G-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-P-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-OPL-D-2G-F	$ 34.00	$ 32.54
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-2P-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-3G-F	$ 48.00	$ 45.94

VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-CLV-OPL-D-3P-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-OPL-D-G-F	$ 18.00	$ 17.23
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-CLV-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-CLV-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-2G-F	$ 173.00	$ 165.59
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-2P-F	$ 188.00	$ 179.95
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-3G-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-3P-F	$ 264.00	$ 252.70
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-G-F	$ 92.00	$ 88.06
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-P-F	$ 100.00	$ 95.72
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-DLD-U-2G-F	$ 230.00	$ 220.15
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-2P-F	$ 245.00	$ 234.51
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-3G-F	$ 323.00	$ 309.17
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-COL-DLD-U-3P-F	$ 344.00	$ 329.27
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-DLD-U-G-F	$ 122.00	$ 116.78
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-P-F	$ 130.00	$ 124.43
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 1 year	V-COL-PLL-U-F	$ 200.00	$ 191.44
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 3 years	V-COL-SSS-U-3G-F	$ 110.88	$ 106.13
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-SSS-U-3P-F	$ 132.00	$ 126.35
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 1 year	V-COL-SSS-U-G-F	$ 42.00	$ 40.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 3 years	V-COL-SSS-U-P-F	$ 50.00	$ 47.86
VMware	TPP L5 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-CLD-D-2G-F	$ 98.00	$ 90.84
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 3 years	V-GMS-CLD-D-2P-F	$ 102.00	$ 94.55
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 1 year	V-GMS-CLD-D-3G-F	$ 138.00	$ 127.92
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 3 years	V-GMS-CLD-D-3P-F	$ 143.00	$ 132.55
VMware	TPP L4 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-CLD-D-G-F	$ 52.00	$ 48.20
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 1 year	V-GMS-CLD-D-P-F	$ 54.00	$ 50.06
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 3 years	V-GMS-CLD-U-2G-F	$ 194.00	$ 179.83
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-2P-F	$ 202.00	$ 187.24
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 3 years	V-GMS-CLD-U-3G-F	$ 272.00	$ 252.13
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-3P-F	$ 283.00	$ 262.33
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 1 year	V-GMS-CLD-U-G-F	$ 103.00	$ 95.48
VMware	U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-P-F	$ 107.00	$ 99.18
VMware	TPP L1 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-2G-F	$ 121.00	$ 112.16
VMware	TPP L4 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-2P-F	$ 125.00	$ 115.87
VMware	TPP L2 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-3G-F	$ 169.00	$ 156.65
VMware	TPP L5 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-3P-F	$ 175.00	$ 162.22
VMware	U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-G-F	$ 64.00	$ 59.32
VMware	TPP L3 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-P-F	$ 66.00	$ 61.18
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-2G-F	$ 239.00	$ 221.54
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 1 year	V-GMS-DLD-U-2P-F	$ 247.00	$ 228.96
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-3G-F	$ 336.00	$ 311.46
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 2 Months	V-GMS-DLD-U-3P-F	$ 346.00	$ 320.73
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-G-F	$ 127.00	$ 117.72
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 1 year	V-GMS-DLD-U-P-F	$ 131.00	$ 121.43

VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 1 year	V-GMS-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 3 year	V-GMS-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 1 year	V-GMS-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 3 year	V-GMS-OPL-D-P-F	$ 42.00	$ 40.20
VMware	TPP L5 U.S. Federal VMware Horizon FLEX Add-On 10 pack (Per Device)	V-GMS-PLL-D-F	$ 50.00	$ 48.87
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-PLL-U-F	$ 100.00	$ 97.73
VMware	TPP L2 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-3G-F	$ 29.04	$ 28.38
VMware	TPP L3 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-3P-F	$ 34.32	$ 33.54
VMware	U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-G-F	$ 11.00	$ 10.75
VMware	TPP L1 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-P-F	$ 13.00	$ 12.71
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-3G-F	$ 55.44	$ 54.18
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 1 year	V-GMS-SSS-U-3P-F	$ 66.00	$ 64.50
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-G-F	$ 21.00	$ 20.52
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-P-F	$ 25.00	$ 24.43
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-HOS-CLD-D-F	$ 24.00	$ 22.97
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-HOS-DLD-D-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch App Catalog: 1 Device for 1 year	V-IDM-CLD-U-2G-F	$ 185.00	$ 177.08
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch App Catalog: 1 Device for 3 years	V-IDM-CLD-U-2P-F	$ 190.00	$ 181.86
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch App Catalog: 1 Device for 1 year	V-IDM-CLD-U-3G-F	$ 259.00	$ 247.91
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-IDM-CLD-U-3P-F	$ 267.00	$ 255.57
VMware	U.S. Federal VMware AirWatch App Catalog Perpetual: 1 Device	V-IDM-CLD-U-G-F	$ 98.00	$ 93.80
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch App Catalog: 1 Device for 3 years	V-IDM-CLD-U-P-F	$ 101.00	$ 96.68
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-IDM-PLL-U-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-3G-F	$ 52.80	$ 50.54
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-3P-F	$ 63.36	$ 60.65
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-IDM-SSS-U-G-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-P-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 1 year	V-INB-CLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 3 years	V-INB-CLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 1 year	V-INB-CLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-CLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Blue Management Suite Perpetual: 1 User	V-INB-CLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 3 years	V-INB-CLD-D-P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-2G-F	$ 68.00	$ 65.09
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-2P-F	$ 70.00	$ 67.00
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-3G-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-3P-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-P-F	$ 37.00	$ 35.42
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Perpetual: 1 Device	V-INB-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-OPL-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-INB-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-3G-F	$ 10.56	$ 10.11

VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-INB-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Teacher Tools Perpetual: 1 Device	V-LTP-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Inbox: 1 Device for 1 year	V-LTP-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Inbox: 1 Device for 3 years	V-LTP-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Inbox: 1 Device for 1 year	V-LTP-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Inbox: 1 Device for 3 years	V-LTP-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 User for 1 year	V-MAW-CLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 User for 3 years	V-MAW-CLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 User for 1 year	V-MAW-CLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-CLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Telecom Perpetual: 1 User	V-MAW-CLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 User for 3 years	V-MAW-CLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MAW-PLL-D-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-3G-F	$ 5.28	$ 5.05
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-3P-F	$ 7.92	$ 7.58
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MAW-SSS-D-G-F	$ 2.00	$ 1.91
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-P-F	$ 3.00	$ 2.87
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 1 year	V-MBM-CLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 3 years	V-MBM-CLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 1 year	V-MBM-CLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-CLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Orange Management Suite Perpetual: 1 User	V-MBM-CLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 3 years	V-MBM-CLD-D-P-F	$ 25.00	$ 23.93

VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-2G-F	$ 68.00	$ 65.09
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-2P-F	$ 70.00	$ 67.00
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-3G-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-3P-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-P-F	$ 37.00	$ 35.42
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Blue Management Suite Perpetual: 1 Device	V-MBM-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-OPL-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MBM-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MBM-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware Collaboration Bundle: 1 User for 1 year	V-MDM-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal Production Support/Subscription for VMware Collaboration Bundle: 1 User for 3 years	V-MDM-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal Production Support/Subscription for VMware Collaboration Bundle: 1 User for 1 year	V-MDM-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware Collaboration Bundle Perpetual: 1 User	V-MDM-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal Basic Support/Subscription for VMware Collaboration Bundle: 1 User for 3 years	V-MDM-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Inbox Perpetual: 1 Device	V-MDM-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MDM-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MDM-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-P-F	$ 13.00	$ 12.44
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-2G-F	$ 115.00	$ 106.60
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-CLD-D-2P-F	$ 121.00	$ 112.16
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-3G-F	$ 162.00	$ 150.17
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-CLD-D-3P-F	$ 169.00	$ 156.65
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-G-F	$ 61.00	$ 56.54
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-P-F	$ 64.00	$ 59.32
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-2G-F	$ 230.00	$ 220.15
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 1 year	V-OMS-CLD-U-2P-F	$ 239.00	$ 228.77
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-3G-F	$ 323.00	$ 309.17

VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 (10 Pack) for 1 year	V-OMS-CLD-U-3P-F	$ 336.00	$ 321.61
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-G-F	$ 122.00	$ 116.78
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 1 year	V-OMS-CLD-U-P-F	$ 127.00	$ 121.56
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-DLD-D-2G-F	$ 138.00	$ 127.92
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-2P-F	$ 143.00	$ 132.55
VMware	U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-3G-F	$ 193.00	$ 178.90
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-3P-F	$ 201.00	$ 186.32
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-DLD-D-G-F	$ 73.00	$ 67.67
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-P-F	$ 76.00	$ 70.45
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 3 years	V-OMS-DLD-U-2G-F	$ 275.00	$ 263.22
VMware	TPP L1 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-2P-F	$ 284.00	$ 271.84
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 3 years	V-OMS-DLD-U-3G-F	$ 386.00	$ 369.47
VMware	TPP L2 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-3P-F	$ 399.00	$ 381.91
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 (10 Pack) for 1 year	V-OMS-DLD-U-G-F	$ 146.00	$ 139.75
VMware	U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced to VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-P-F	$ 151.00	$ 144.53
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-OPL-D-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 2 Months	V-OMS-OPL-D-2P-F	$ 98.00	$ 93.80
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-OPL-D-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 2 Months	V-OMS-OPL-D-3P-F	$ 138.00	$ 132.09
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-OPL-D-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-OPL-D-P-F	$ 52.00	$ 49.77
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 2 Months	V-OMS-PLL-D-F	$ 70.00	$ 68.41
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-PLL-U-F	$ 140.00	$ 134.01
VMware	U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-SSS-D-3G-F	$ 39.60	$ 38.70
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-SSS-D-3P-F	$ 47.52	$ 46.44
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 3 years	V-OMS-SSS-D-G-F	$ 15.00	$ 14.66
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 3 years	V-OMS-SSS-D-P-F	$ 18.00	$ 17.59
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-3G-F	$ 76.56	$ 73.28
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-3P-F	$ 92.40	$ 88.44
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-SSS-U-G-F	$ 29.00	$ 27.76
VMware	U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal AirWatch by VMware Accelerated Deployment Add-On One Time Fee	V-PS-ACCELERATE-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware AirWatch Per App Tunneling Configuration One Time Fee	V-PS-APP-VPN-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Application Server Migration	V-PS-APSV-MG-SP-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal VMware AirWatch Reports Server Configuration and Deployment One Time Fee	V-PS-AW-RPT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Telecom Module Deployment One Time Fee	V-PS-AWT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Video Deployment One Time Fee	V-PS-AWV-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Blue Management Suite Cloud Deployment Fee One Time Fee	V-PS-BMS-CLD-SP-F	$ 4,500.00	$ 4,397.98
VMware	U.S. Federal VMware AirWatch Blue Management Suite On Premise Deployment Fee One Time Fee	V-PS-BMS-OP-SP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal AirWatch by VMware Blue Management Suite On-Premise - Includes 3 days On-Site	V-PS-BMS-OPL-3OS-F	$ 9,800.00	$ 9,577.83
VMware	U.S. Federal AirWatch by VMware Blue Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-BMS-OPL-RSS-F	$ 7,250.00	$ 7,085.64
VMware	U.S. Federal VMware AirWatch Database Server Migration	V-PS-DBSV-MG-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Device Enrollment Program (DEP) Configuration and Deployment One Time Fee	V-PS-DEP-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated Environment Setup One Time Fee / Environment	V-PS-DHE-SET-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated UAT Environment 1 Year Fee / Device	V-PS-DHE-UAT-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Disaster Recovery Set-up Fee	V-PS-DR-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Cloud Connector (ACC) Configuration and Deployment - Enterprise Integration One Time Fee	V-PS-ENT-ACC-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-PS-ENT-SUP-GEO-F	$ 25,000.00	$ 23,929.47
VMware	U.S. Federal AirWatch by VMware End User On-Boarding Video	V-PS-EU-OBV-F	$ 1,200.00	$ 1,172.80

VMware	U.S. Federal VMware AirWatch Enterprise Gold SaaS Cloud Deployment up to 100000 devices One Time Fee	V-PS-GLD-CLD-SP-F	$ 37,500.00	$ 36,649.87
VMware	U.S. Federal VMware AirWatch Enterprise Gold On Premise Deployment up to 100000 devices One Time Fee	V-PS-GLD-OP-SP-F	$ 50,000.00	$ 48,866.50
VMware	U.S. Federal VMware AirWatch Green Management Suite Lite Cloud Deployment Fee One Time Fee	V-PS-GMCL-LITE-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Green Management Suite Lite On Premise Deployment Fee One Time Fee	V-PS-GMOP-LITE-F	$ 1,750.00	$ 1,710.33
VMware	U.S. Federal VMware AirWatch Green Management Suite Cloud Deployment Fee One Time Fee	V-PS-GMS-CLD-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Green Management Suite On Premise Deployment Fee One Time Fee	V-PS-GMS-OP-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal AirWatch by VMware Green Management Suite On-Premise - Includes 2 days On-Site	V-PS-GMS-OPL-2OS-F	$ 5,450.00	$ 5,326.45
VMware	U.S. Federal AirWatch by VMware Green Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-GMS-OPL-RSS-F	$ 3,250.00	$ 3,176.32
VMware	U.S. Federal VMware AirWatch High Availability Set-up One Time Fee	V-PS-HA-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Health Check One Time Fee	V-PS-HC-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Professional Services - 1 hour of support services One Time Fee	V-PS-HR-PS-F	$ 150.00	$ 146.60
VMware	U.S. Federal AirWatch by VMware Browser Deployment Fee One Time Fee	V-PS-MBM-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal AirWatch by VMware AirWatch Content Locker Collaborate Add-On for K12+MAG Management Suite Deployment One Time Fee	V-PS-MCC-BMS-SP-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal AirWatch by VMware AirWatch Content Collaborate Add-On for Green/Orange Deployment Fee One Time Fee	V-PS-MCC-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Mobile Content Management Only Cloud Deployment One Time Fee	V-PS-MCM-CLD-SP-F	$ 2,000.00	$ 1,954.66
VMware	U.S. Federal VMware AirWatch Mobile Content Management Only On Premise Deployment One Time Fee	V-PS-MCM-OP-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware AirWatch Content View Cloud Deployment Fee One Time Fee	V-PS-MCV-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Advanced Migration Configuration and Deployment On Premise Deployment Fee One Time Fee	V-PS-MIG-ADV-OP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal AirWatch by VMware Advanced Migration Configuration and Deployment Cloud One Time Fee	V-PS-MIG-ADV-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware AirWatch Basic Migration Configuration and Deployment On Premise Deployment Fee One Time Fee	V-PS-MIG-BASIC-OP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal AirWatch by VMware Basic Migration Configuration and Deployment Cloud Deployment One Time Fee	V-PS-MIG-BASIC-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Rugged Device Configuration and Deployment Add-On One Time Fee	V-PS-MS-ADDONRG-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Rugged Device Cloud Configuration and Deployment One Time Fee	V-PS-MS-CLDSPRG-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Rugged Device On Premise Configuration and Deployment One Time Fee	V-PS-MS-OP-SPRG-SP-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware AirWatch Orange Management Suite Cloud Deployment Fee One Time Fee	V-PS-OMS-CLD-SP-F	$ 2,000.00	$ 1,954.66
VMware	U.S. Federal VMware AirWatch Orange Management Suite On Premise Deployment Fee One Time Fee	V-PS-OMS-OP-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal AirWatch by VMware Orange Management Suite On-Premise - Includes 2 days On-Site	V-PS-OMS-OPL-2OS-F	$ 6,200.00	$ 6,059.45
VMware	U.S. Federal AirWatch by VMware Orange Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-OMS-OPL-RSS-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware AirWatch On Premise to Dedicated Deployment One Time Fee	V-PS-OP2-DHS-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal AirWatch by VMware On-Premise Weekend Upgrades and Off-Hours Requiring Same Region One Time Fee	V-PS-OPL-WUOH-F	$ 3,700.00	$ 3,616.12
VMware	U.S. Federal VMware AirWatch PKI Certificate Advanced Configuration and Deployment One Time Fee	V-PS-PKI-ADV-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch PKI Certificate Basic Configuration and Deployment One Time Fee	V-PS-PKI-BASIC-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch PowerShell Configuration and Deployment One Time Fee	V-PS-PWR-SHELL-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal AirWatch Socialcast Cloud Deployment One Time Fee	V-PS-SC-CLD-SP-F	$ 1,800.00	$ 1,759.19
VMware	U.S. Federal AirWatch by VMware SocialCast Dedicated SaaS Setup Fee One Time Fee	V-PS-SC-DSAAS-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal AirWatch Socialcast On Premise Deployment One Time Fee	V-PS-SC-OP-SP-F	$ 4,200.00	$ 4,104.79
VMware	U.S. Federal AirWatch by VMware SaaS SEG and MAG Upgrade	V-PS-SEG-MAG-UG-F	$ 800.00	$ 781.86
VMware	U.S. Federal AirWatch by VMware SaaS SEG and MAG Weekend and Same Region Off-Hours Upgrade	V-PS-SEG-MAG-WR-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal VMware AirWatch Secure Email Gateway (SEG) Configuration and Deployment One Time Fee	V-PS-SEG-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Enterprise Silver SaaS Cloud Deployment up to 50000 devices One Time Fee	V-PS-SLV-CLD-SP-F	$ 20,000.00	$ 19,546.60
VMware	U.S. Federal VMware AirWatch Enterprise Silver On Premise Deployment up to 50000 devices One Time Fee	V-PS-SLV-OP-SP-F	$ 25,000.00	$ 24,433.25
VMware	U.S. Federal VMware AirWatch Professional Services - 8 hours of support services One Time Fee	V-PS-SP-DAY-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Standby Support (Monday - Friday) One Time Fee	V-PS-STBS-WD-PS-F	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal VMware AirWatch Standby Support (Weekend) One Time Fee	V-PS-STBS-WE-PS-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Incident Support Package 5 pack	V-PS-SUPP-INC-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-PS-TAM-F	$ 69,995.00	$ 66,997.73
VMware	U.S. Federal VMware AirWatch Professional Services Travel and Expense - daily One Time Fee	V-PS-TE-AW-F	$ 610.00	$ 596.17
VMware	U.S. Federal VMware AirWatch Teacher Tools Deployment One Time Fee	V-PS-TT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Upgrade from Green Management Suite to Orange Management Suite Deployment (Cloud or On Premise) One Time Fee	V-PS-UPG-GM-OM-SP-F	$ 500.00	$ 488.66

VMware	U.S. Federal VMware AirWatch Dedicated Cloud Upgrade off-hours One Time Fee	V-PS-UPGR-OFFHOURS-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Upgrade Services for On Premise Deployments Fee One Time Fee	V-PS-UPGR-STD-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware Collaborate Bundle Cloud Deployment One Time Fee	V-PS-VCB-CLD-SP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware Collaborate Bundle On Premise Deployment One time Fee	V-PS-VCB-OP-SP-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal VMware Identity Manager Shared Cloud Deployment One Time Fee	V-PS-VIDM-CLD-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware Identity Manager On Premise Deployment One Time Fee	V-PS-VIDM-OP-SP-F	$ 1,800.00	$ 1,759.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Cloud Deployment Fee One Time Fee	V-PS-YMS-CLD-SP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite On Premise Deployment Fee One Time Fee	V-PS-YMS-OP-SP-F	$ 6,500.00	$ 6,352.64
VMware	U.S. Federal AirWatch by VMware Yellow Management Suite On-Premise - Includes 3 days On-Site	V-PS-YMS-OPL-3OS-F	$ 11,050.00	$ 10,799.50
VMware	U.S. Federal AirWatch by VMware Yellow Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-YMS-OPL-RSS-F	$ 8,500.00	$ 8,307.30
VMware	U.S. Federal VMware Identity Manager Advanced Edition SaaS Deployment One Time Fee	V-PSVIDM-ADVCLD-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware Identity Manager Advanced Edition On-Premises Deployment One Time Fee	V-PSVIDM-ADVOP-SP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-DLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-PTR-DLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-DLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 1 year	V-PTR-PLL-D-F	$ 25.00	$ 23.93
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 3 years	V-PTR-SSS-D-3G-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-SSS-D-3P-F	$ 15.84	$ 15.16
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 1 year	V-PTR-SSS-D-G-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 3 years	V-PTR-SSS-D-P-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 User for 1 year	V-RUG-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 User for 3 years	V-RUG-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 User for 1 year	V-RUG-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware AirWatch Video Perpetual: 1 User	V-RUG-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 User for 3 years	V-RUG-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-RUG-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-3G-F	$ 29.04	$ 27.80

VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-RUG-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-2G-F	$ 59.00	$ 56.47
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-2P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-3G-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-3P-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-G-F	$ 31.00	$ 29.67
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-DLD-U-2G-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-2P-F	$ 89.00	$ 85.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-3G-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware AirWatch Mobile Browser Perpetual: 1 Device	V-SCT-DLD-U-3P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-DLD-U-G-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 1 year	V-SCT-PLL-U-F	$ 90.00	$ 86.15
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 3 years	V-SCT-SSS-U-3G-F	$ 50.16	$ 48.01
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-SSS-U-3P-F	$ 60.72	$ 58.12
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 1 year	V-SCT-SSS-U-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 3 years	V-SCT-SSS-U-P-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-CLD-U-2G-F	$ 47.00	$ 44.99
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-2P-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-3G-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-CLD-U-3P-F	$ 69.00	$ 66.05
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-CLD-U-G-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-P-F	$ 26.00	$ 24.89
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-DLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-DLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-DLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-DLD-U-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-2P-F	$ 94.00	$ 89.97
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-DLD-U-3P-F	$ 132.00	$ 126.35
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-DLD-U-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-P-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Laptop Management Suite Perpetual: 1 Device	V-TEL-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-OPL-D-G-F	$ 12.00	$ 11.49

VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 1 year	V-TEL-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 1 year	V-TEL-PLL-U-F	$ 40.00	$ 38.29
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 3 years	V-TEL-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 1 year	V-TEL-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 3 years	V-TEL-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 3 years	V-TEL-SSS-U-3G-F	$ 21.12	$ 20.22
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-SSS-U-3P-F	$ 26.40	$ 25.27
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 1 year	V-TEL-SSS-U-G-F	$ 8.00	$ 7.66
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 3 years	V-TEL-SSS-U-P-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-DLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-DLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-DLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-OPL-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Perpetual: 1 User	V-TTS-OPL-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-OPL-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 1 year	V-TTS-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 3 years	V-TTS-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 1 year	V-TTS-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 3 years	V-TTS-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-BU-CLD-U-G-F	$ 83.50	$ 77.40
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 3 years	V-UG-BU-CLD-U-P-F	$ 87.00	$ 80.64
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-BU-DLD-U-G-F	$ 97.00	$ 89.91
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 3 years	V-UG-BU-DLD-U-P-F	$ 100.00	$ 92.70
VMware	U.S. Federal VMware AirWatch Enterprise Support 1 Year Fee per Geography or Business Unit	V-UG-BU-PLL-U-F	$ 99.00	$ 96.76
VMware	U.S. Federal VMware AirWatch Technical Account Manager can be purchased by AirWatch Production or Enterprise Customers	V-UG-BU-SSS-U-G-F	$ 21.00	$ 20.52
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-BU-SSS-U-P-F	$ 25.00	$ 24.43
VMware	U.S. Federal VMware Identity Manager Advanced Edition Perpetual: 1 User	V-UG-BY-CLD-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-BY-CLD-D-P-F	$ 40.50	$ 38.77
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-BY-CLD-U-G-F	$ 78.00	$ 74.66
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-BY-CLD-U-P-F	$ 81.50	$ 78.01
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-BY-DLD-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-BY-DLD-D-P-F	$ 40.50	$ 37.54
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-BY-DLD-U-G-F	$ 78.00	$ 74.66
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-BY-DLD-U-P-F	$ 81.50	$ 75.55

VMware	U.S. Federal Basic Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 1 year	V-UG-BY-OPL-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices Perpetual: 1 Device	V-UG-BY-OPL-D-P-F	$ 40.50	$ 38.77
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-BY-PLL-D-F	$ 44.00	$ 43.00
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - On Premise (Includes Basic Support/	V-UG-BY-SSS-D-G-F	$ 9.00	$ 8.80
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Suppo	V-UG-BY-SSS-D-P-F	$ 11.00	$ 10.75
VMware	U.S. Federal Production Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 1 year	V-UG-GB-CLD-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 1 year	V-UG-GB-CLD-D-P-F	$ 28.50	$ 27.28
VMware	U.S. Federal VMware Identity Manager Advanced Edition 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GB-CLD-U-G-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GB-CLD-U-P-F	$ 57.00	$ 54.56
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GB-DLD-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GB-DLD-D-P-F	$ 28.50	$ 26.42
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GB-DLD-U-G-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GB-DLD-U-P-F	$ 57.00	$ 52.84
VMware	U.S. Federal VMware Identity Manager Advanced Edition 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GB-OPL-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 3 years	V-UG-GB-OPL-D-P-F	$ 28.50	$ 27.28
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-GB-PLL-D-F	$ 44.00	$ 43.00
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-GB-SSS-D-G-F	$ 9.00	$ 8.80
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GB-SSS-D-P-F	$ 11.00	$ 10.75
VMware	U.S. Federal Basic Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 3 years	V-UG-GO-CLD-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 1 year	V-UG-GO-CLD-D-P-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware Identity Manager Advanced Edition 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GO-CLD-U-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-GO-CLD-U-P-F	$ 22.00	$ 21.06
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GO-DLD-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GO-DLD-D-P-F	$ 11.00	$ 10.20
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-GO-DLD-U-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Content Locker View Perpetual: 1 Device	V-UG-GO-DLD-U-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal VMware Identity Manager Advanced Edition 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GO-OPL-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GO-OPL-D-P-F	$ 11.00	$ 10.53
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-PLL-D-F	$ 22.00	$ 21.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-SSS-D-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-SSS-D-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal Production Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 3 years	V-UG-GY-CLD-D-G-F	$ 66.00	$ 63.17
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 3 years	V-UG-GY-CLD-D-P-F	$ 69.50	$ 66.52
VMware	U.S. Federal VMware Identity Manager Advanced Edition 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GY-CLD-U-G-F	$ 132.00	$ 126.35
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-GY-CLD-U-P-F	$ 138.50	$ 132.57
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-D-G-F	$ 64.00	$ 59.32
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-D-P-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-U-G-F	$ 132.00	$ 122.36
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-GY-DLD-U-P-F	$ 138.50	$ 128.38
VMware	U.S. Federal VMware Identity Manager Advanced Edition 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GY-OPL-D-G-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GY-OPL-D-P-F	$ 69.50	$ 66.52
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Dedicated Cloud (Includes SaaS Ba	V-UG-GY-PLL-D-F	$ 88.00	$ 86.01
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Dedicated Cloud (Includes SaaS Ba	V-UG-GY-SSS-D-G-F	$ 18.00	$ 17.59
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Dedicated Clo	V-UG-GY-SSS-D-P-F	$ 22.00	$ 21.50
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-MU-CLD-U-G-F	$ 56.00	$ 51.91
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-MU-CLD-U-P-F	$ 58.50	$ 54.23
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-MU-DLD-U-G-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-MU-DLD-U-P-F	$ 71.50	$ 66.28
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-MU-PLL-U-F	$ 55.00	$ 53.75

VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Support/S	V-UG-MU-SSS-U-G-F	$ 12.00	$ 11.73
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Sup	V-UG-MU-SSS-U-P-F	$ 14.00	$ 13.68
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 1 year	V-UG-MY-CLD-D-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-MY-CLD-D-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-MY-DLD-D-G-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 1 year	V-UG-MY-DLD-D-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 1 year	V-UG-MY-OPL-D-G-F	$ 46.00	$ 44.03
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-MY-OPL-D-P-F	$ 48.50	$ 46.42
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - On Premise (Includes Basic Suppor	V-UG-MY-PLL-D-F	$ 66.00	$ 64.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Support	V-UG-MY-SSS-D-G-F	$ 14.00	$ 13.68
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Sup	V-UG-MY-SSS-D-P-F	$ 17.00	$ 16.61
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 3 years	V-UG-OB-CLD-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-OB-CLD-D-P-F	$ 17.50	$ 16.75
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OB-CLD-U-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OB-CLD-U-P-F	$ 35.00	$ 32.44
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-OB-DLD-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 1 year	V-UG-OB-DLD-D-P-F	$ 17.50	$ 16.22
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OB-DLD-U-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 3 years	V-UG-OB-DLD-U-P-F	$ 35.00	$ 32.44
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OB-OPL-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OB-OPL-D-P-F	$ 17.50	$ 16.75
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basi	V-UG-OB-PLL-D-F	$ 22.00	$ 21.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basi	V-UG-OB-SSS-D-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal Upgrade: VMware AirWatch Orange Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic Su	V-UG-OB-SSS-D-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-OU-CLD-U-G-F	$ 67.00	$ 62.11
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-OU-CLD-U-P-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OU-DLD-U-G-F	$ 80.50	$ 74.62
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OU-DLD-U-P-F	$ 82.50	$ 76.47
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-OU-PLL-U-F	$ 77.00	$ 75.25
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-OU-SSS-U-G-F	$ 16.00	$ 15.64
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate - Shared Cloud (Includes SaaS Basi	V-UG-OU-SSS-U-P-F	$ 19.00	$ 18.57
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 3 years	V-UG-OY-CLD-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-CLD-D-P-F	$ 56.00	$ 51.91
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-OY-CLD-U-G-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-OY-CLD-U-P-F	$ 116.50	$ 107.99
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-OY-DLD-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-DLD-D-P-F	$ 58.50	$ 54.23
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OY-DLD-U-G-F	$ 111.00	$ 106.25
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 3 years	V-UG-OY-DLD-U-P-F	$ 116.50	$ 107.99
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-OPL-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OY-OPL-D-P-F	$ 58.50	$ 55.99
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate - Dedicated Cloud (Includes SaaS B	V-UG-OY-PLL-D-F	$ 66.00	$ 64.50
VMware	U.S. Federal Upgrade: VMware AirWatch Orange Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic Su	V-UG-OY-SSS-D-G-F	$ 14.00	$ 13.68
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Product	V-UG-OY-SSS-D-P-F	$ 17.00	$ 16.61
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-TU-CLD-U-G-F	$ 14.50	$ 13.44
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping Perpetual: 1 Device	V-UG-TU-CLD-U-P-F	$ 14.50	$ 13.44
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptio	V-UG-TU-DLD-U-G-F	$ 27.50	$ 25.49
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-TU-DLD-U-P-F	$ 27.50	$ 25.49
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptio	V-UG-TU-PLL-U-F	$ 22.00	$ 21.50

VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-TU-SSS-U-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-TU-SSS-U-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate Perpetual: 1 Device	V-UG-VC-CLD-D-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-VC-CLD-D-P-F	$ 22.00	$ 21.06
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-VC-DLD-D-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-VC-DLD-D-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-VC-PLL-D-F	$ 33.00	$ 32.25
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-VC-SSS-D-G-F	$ 7.00	$ 6.84
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - On Premise (Includes Basic Support/S	V-UG-VC-SSS-D-P-F	$ 8.00	$ 7.82
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-VU-CLD-U-G-F	$ 33.00	$ 30.59
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 1 year	V-UG-VU-CLD-U-P-F	$ 34.00	$ 31.52
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-VU-DLD-U-G-F	$ 46.00	$ 42.64
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 1 year	V-UG-VU-DLD-U-P-F	$ 47.50	$ 44.03
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-VU-PLL-U-F	$ 33.00	$ 32.25
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated Environment for Perpetual Licenses: 1 Device for 1 year	V-UG-VU-SSS-U-G-F	$ 7.00	$ 6.84
VMware	U.S. Federal VMware AirWatch Cloud - Shared Environment for Perpetual Licenses: 1 Device for 1 year	V-UG-VU-SSS-U-P-F	$ 8.00	$ 7.82
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-YU-CLD-U-G-F	$ 122.00	$ 113.09
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-YU-CLD-U-P-F	$ 127.50	$ 118.19
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptio	V-UG-YU-DLD-U-G-F	$ 135.50	$ 125.60
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-YU-DLD-U-P-F	$ 141.00	$ 130.70
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - On Premise (I	V-UG-YU-PLL-U-F	$ 143.00	$ 139.76
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Shared Cloud	V-UG-YU-SSS-U-G-F	$ 30.00	$ 29.32
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite. Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-YU-SSS-U-P-F	$ 36.00	$ 35.18
VMware	U.S. Federal Basic Support/Subscription for VMware Socialcast: 1 User for 1 year	V-VID-CLD-D-2G-F	$ 59.00	$ 56.47
VMware	U.S. Federal Production Support/Subscription for VMware Socialcast: 1 User for 3 years	V-VID-CLD-D-2P-F	$ 61.00	$ 58.39
VMware	U.S. Federal Production Support/Subscription for VMware Socialcast: 1 User for 1 year	V-VID-CLD-D-3G-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-CLD-D-3P-F	$ 85.00	$ 81.36
VMware	U.S. Federal VMware Socialcast Perpetual: 1 User	V-VID-CLD-D-G-F	$ 31.00	$ 29.67
VMware	U.S. Federal Basic Support/Subscription for VMware Socialcast: 1 User for 3 years	V-VID-CLD-D-P-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-2G-F	$ 115.00	$ 110.08
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-2P-F	$ 119.00	$ 113.90
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-3G-F	$ 162.00	$ 155.06
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-3P-F	$ 167.00	$ 159.85
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-G-F	$ 61.00	$ 58.39
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-P-F	$ 63.00	$ 60.30
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-2G-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-2P-F	$ 83.00	$ 79.45
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-3G-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-3P-F	$ 117.00	$ 111.99
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-G-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-P-F	$ 44.00	$ 42.12
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-DLD-U-2G-F	$ 160.00	$ 153.15
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-2P-F	$ 164.00	$ 156.98
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-3G-F	$ 225.00	$ 215.37
VMware	U.S. Federal VMware AirWatch Mobile Device Perpetual: 1 Device	V-VID-DLD-U-3P-F	$ 230.00	$ 220.15
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-DLD-U-G-F	$ 85.00	$ 81.36
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-P-F	$ 87.00	$ 83.27
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-OPL-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-2P-F	$ 38.00	$ 36.37

VMware	U.S. Federal VMware Socialcast 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Printer Perpetual: 1 Device	V-VID-OPL-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-OPL-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-VID-PLL-D-F	$ 30.00	$ 28.72
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Printer: 1 Device for 1 year	V-VID-PLL-U-F	$ 60.00	$ 57.43
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-3G-F	$ 15.84	$ 15.16
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-3P-F	$ 21.12	$ 20.22
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-VID-SSS-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-P-F	$ 8.00	$ 7.66
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Printer: 1 Device for 3 years	V-VID-SSS-U-3G-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-SSS-U-3P-F	$ 39.60	$ 37.90
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Printer: 1 Device for 1 year	V-VID-SSS-U-G-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Printer: 1 Device for 3 years	V-VID-SSS-U-P-F	$ 15.00	$ 14.36
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 1 year	V-YMS-CLD-D-2G-F	$ 211.00	$ 201.96
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 3 years	V-YMS-CLD-D-2P-F	$ 220.00	$ 210.58
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 1 year	V-YMS-CLD-D-3G-F	$ 296.00	$ 283.32
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-D-3P-F	$ 309.00	$ 295.77
VMware	U.S. Federal VMware AirWatch Green Management Suite Perpetual: 1 User	V-YMS-CLD-D-G-F	$ 112.00	$ 107.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 3 years	V-YMS-CLD-D-P-F	$ 117.00	$ 111.99
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-U-2G-F	$ 420.00	$ 402.02
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-2P-F	$ 439.00	$ 420.20
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-3G-F	$ 589.00	$ 563.78
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-CLD-U-3P-F	$ 616.00	$ 589.62
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-U-G-F	$ 223.00	$ 213.45
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-P-F	$ 233.00	$ 223.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-2G-F	$ 234.00	$ 223.98
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-2P-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-3G-F	$ 328.00	$ 313.95
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-3P-F	$ 341.00	$ 326.40
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-G-F	$ 124.00	$ 118.69
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-P-F	$ 129.00	$ 123.48
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-DLD-U-2G-F	$ 465.00	$ 445.09
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-2P-F	$ 484.00	$ 463.27
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-3G-F	$ 653.00	$ 625.04
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-DLD-U-3P-F	$ 679.00	$ 649.92
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-DLD-U-G-F	$ 247.00	$ 236.42
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-P-F	$ 257.00	$ 245.99
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-OPL-D-2G-F	$ 188.00	$ 179.95
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-2P-F	$ 198.00	$ 189.52
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - Extra Person	EDU-VICM5-XP-F	$ 2,750.00	$ 2,687.66
VMware	Application Virtualization with VMware ThinApp [V5.0] - Open Enrollment	EDU-THINAPP5-OE-F	$ 825.00	$ 806.30
VMware	Application Virtualization with VMware ThinApp [V5.0] - On Site	EDU-THINAPP5-OS-F	$ 6,875.00	$ 6,719.14
VMware	Application Virtualization with VMware ThinApp [V5.0] - Extra Person	EDU-THINAPP5-XP-F	$ 688.00	$ 672.40
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Open Enrollment	EDU-VCACEXT52-OE-F	$ 1,645.00	$ 1,607.71
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Onsite	EDU-VCACEXT52-OS-F	$ 13,750.00	$ 13,438.29
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Extra Person	EDU-VCACEXT52-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal Using VMware vCenter Lab Manager - Open Enrollment	EDU-LM4-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal Using VMware vCenter Lab Manager - On Site	EDU-LM4-OS-F	$ 6,875.00	$ 6,719.14

VMware	U.S. Federal Using VMware vCenter Lab Manager - Extra Person	EDU-LM4-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 1-150	SVC-CR-0-F	$ 100.00	$ 97.73
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 1-150.	SVC-CR-0-SSS-F	$ 100.00	$ 97.73
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 151-600	SVC-CR-10-F	$ 90.00	$ 87.96
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 151-600.	SVC-CR-10-SSS-F	$ 90.00	$ 87.96
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 601-1200	SVC-CR-15-F	$ 85.00	$ 83.07
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 601-1200.	SVC-CR-15-SSS-F	$ 85.00	$ 83.07
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 1201+	SVC-CR-20-F	$ 80.00	$ 78.19
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 1201+	SVC-CR-20-SSS-F	$ 80.00	$ 78.19
VMware	U.S. Federal Socialcast Configuration and Integration Design - On Premises	CON-SC-CIDOP-FF-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal Socialcast Assigned Client Account Representative	CON-SC-ACAR-FF-F	$ 30,000.00	$ 29,319.90
VMware	U.S. Federal Socialcast Reach System Integration	CON-SC-RSI-FF-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal Socialcast Single Sign On Configuration	CON-SC-SSOC-FF-F	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal Socialcast Custom Theme Integration	CON-SC-CTI-FF-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-3G-F	$ 264.00	$ 252.70
VMware	U.S. Federal VMware AirWatch Orange Management Suite Perpetual: 1 Device	V-YMS-OPL-D-3P-F	$ 278.00	$ 266.10
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-OPL-D-G-F	$ 100.00	$ 95.72
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-P-F	$ 105.00	$ 100.50
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-PLL-D-F	$ 130.00	$ 124.43
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 1 year	V-YMS-PLL-U-F	$ 260.00	$ 248.87
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-YMS-SSS-D-3G-F	$ 71.28	$ 68.23
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-YMS-SSS-D-3P-F	$ 87.12	$ 83.39
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-SSS-D-G-F	$ 27.00	$ 25.84
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-YMS-SSS-D-P-F	$ 33.00	$ 31.59
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 3 years	V-YMS-SSS-U-3G-F	$ 145.20	$ 138.98
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-SSS-U-3P-F	$ 171.60	$ 164.25
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 1 year	V-YMS-SSS-U-G-F	$ 55.00	$ 52.64
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 3 years	V-YMS-SSS-U-P-F	$ 65.00	$ 62.22
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - On Premise (I	V-YMS-WKS-MF-2M-SSS-F	$ 10.84	$ 10.59
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Shared Cloud	V-YMS-WKS-MF-3Y-SSS-F	$ 171.60	$ 167.71
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate Subscription - Shared Cloud (Includ	V-YMS-WKS-MF-SSS-F	$ 65.00	$ 63.53
VMware	U.S. Federal VMware vCloud Air Accelerator	CON-VCA-ACL-F	$ 19,035.00	$ 18,603.48
VMware	U.S. Federal VMware Desktop Viritualization Health Check	CON-VDI-HC-S-F	$ 24,406.60	$ 23,853.30

carahsoft

CARAHSOFT'S RESPONSE TO THE

State of Utah
NASPO ValuePoint

REQUEST FOR PROPOSAL

NASPO ValuePoint Master Agreement for Cloud Solutions

SOLICITATION NO. CH16012

Technical Proposal

Thursday
March 10, 2015

CARAHSOFT TECHNOLOGY CORP.
1860 MICHAEL FARADAY DRIVE, SUITE 100
RESTON, VA 20190

888.66.CARAH | WWW.CARAHSOFT.COM

March 10, 2015

State of Utah Division of Purchasing
3150 State Office Building
Capitol Hill
Salt Lake City, Utah 84114

Re: Carahsoft's Response to the State of Utah's Request for Proposal for NASPO ValuePoint Master Agreement for Cloud Solutions, Solicitation # CH16012.

Dear Mr. Hughes,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of Utah's Request for Proposals/Q/Information for Project Description.

5.2.1	Carahsoft Technology Corporation understands that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.
5.2.2	When writing this response Carahsoft utilized the OEMs being proposed as a part of this response to assist in preparing this response. Staff responsible for creating this proposal include Robert R. Moore – Vice President, Jack Dixon – Contract Specialist, & David Holl – Proposal Coordinator.
5.2.3	Carahsoft Technology Corporation is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.
5.2.4	Carahsoft Technology Corporation acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.
5.2.5	Carahsoft Technology Corporation is including an all-encompassing list of solutions in this response which covers the SaaS, PaaS, & IaaS categories. Services completion/deployment will vary based on manufacturer but will utilize either the manufacturers own integration policies and procedures or a third party subcontractor specializing in servicing the manufacturers' specific solution.
5.2.6	Carahsoft can provide varying levels of data risk support based on customer requirements, manufacturer, and solution type. Please see our response to Attachment H for further detail.

Please feel free to contact me directly at 703.871.8504/Robert.Moore@carahsoft.com or Jack Dixon at 703.230.7545/Jack.Dixon@carahsoft.com with any questions or communications that will assist the Agency in the evaluation of our response. This proposal is valid for 90 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Robert R. Moore
Vice President

TABLE OF CONTENTS

RFP Signature Page 1
Acknowledgement of Amendments 4
Executive Summary 6
Prime Contractor: Carahsoft Technology Corp. 6
Mandatory Minimums 8
Business Profile 12
Organizations Profile 21
Technical Response 23
Confidential, Protected, or Proprietary Information 183
Exceptions and/or Additions to the Standard Terms and Conditions 185
In Summary 186
Supplemental Information 187

RFP SIGNATURE PAGE

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.

Please find below Carahsoft's RFP Signature Page below.

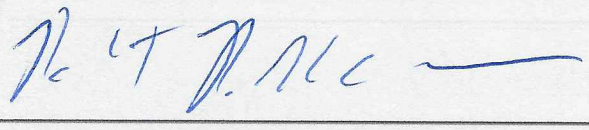
State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number	
Carahsoft Technology Corporation	52-2189693	9721863-0143	
Ordering Address	**City**	**State**	**Zip Code**
1860 Michael Faraday Drive, Suite 100	Reston	VA	20190
Remittance Address (if different from ordering address)	**City**	**State**	**Zip Code**
1860 Michael Faraday Drive, Suite 100	Reston	VA	20190
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person: Robert R. Moore		
Telephone Number (include area code): 703.871.8504	Fax Number (include area code): 703.871.8505		
Company's Internet Web Address: www.carahsoft.com	Email Address: robert.moore@carahsoft.com		
Offeror's Authorized Representative's Signature			
Type or Print Name: Robert R. Moore			
Position or Title of Authorized Representative: Vice President			
Date: 3/10/2016			

State of Utah
Request for Proposal

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number	
Carahsoft Technology Corporation	52-2189693	9721863-0143	
Ordering Address 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Remittance Address (if different from ordering address) 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Type [X] Corporation [ ] Partnership [ ] Proprietorship [ ] Government	Company Contact Person Robert R. Moore		
Telephone Number (include area code) 703.871.8504	Fax Number (include area code) 703.871.8505		
Company's Internet Web Address www.Carahsoft.com	Email Address Robert.Moore@Carahsoft.com		
Discount Terms (for prompt payment discounts): Not Applicable	Days Required for Delivery After Receipt of Order (see attached for any required minimums)		

By submitting a proposal in response to this RFP, the Offeror acknowledges and agrees that the specifications, terms and conditions, or other elements of the RFP are not ambiguous, confusing, contradictory, unduly restrictive, erroneous, or anticompetitive. The Offeror further acknowledges that it has read this RFP, along with any attached or referenced documents, and this document, including the General Provisions.

Offeror's Authorized Representative's Signature	Date
	3/10/2016
Type or Print Name Robert R. Moore	Position or Title Vice President

NOTICE

ACKNOWLEDGEMENT OF AMENDMENTS

Please find below Carahsoft's Acknowledgement of Amendments.

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 10, 2016.

By signing below, the Offeror attest to reviewing the documents listed above.

Carahsoft Technology Corporation
Offeror

Representative Signature

EXECUTIVE SUMMARY

The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.

Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corporation understands that the State of Utah & NASPO ValuePoint is seeking a Master Agreement for Cloud Solutions.

Carahsoft has assembled a team from our vast portfolio of over 200 hundred vendors that includes our premiere network of cloud solutions, resellers, and subcontractors as the best solution to meet the State of Utah's requirements. The intent of our proposal is to deliver the highest value proposition at the lowest possible cost to the State of Utah, NASPO ValuePoint, & all participating entities for the acquisition of cloud solutions. Carahsoft understands the need for high quality cloud based service providers that have the ability to provide a menu of cloud solution offerings. Carahsoft's superior contract management and network of Cloud Solution Providers will ultimately increase the State & Participating Entities overall efficiency, reduce costs, improve operational scalability, provide business continuity, increase collaboration efficiencies, and all for expanded flexibility.

Carahsoft Technology Corp. is an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading software license GSA resellers.

VENDOR RELATIONSHIPS – Just as each state, territory, and participating entity is unique in how they employ cloud solutions, Carahsoft's cloud offering follows a unique business model focusing on providing superior sales and marketing execution, a track record of success, high integrity, and a focus on strategic vendor relationships.

PROVEN EXECUTION (Growth and Experience of Sales) – Carahsoft has been supporting the IT needs of Government and Education Customers for more than 12 years. Our Public Sector Sales Team supports the Government, Education, and Healthcare vertical markets and is an enormous component of Carahsoft's ongoing and continued growth. In 2014, Carahsoft had revenues of over $2B in the public sector market. Our State & Local Government Sales Force is solely dedicated to supporting the unique needs of Higher Education, K- 12 Schools, State Government, and Local Government customers.

CONTRACT VEHICLES – Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Carahsoft holds statewide contracts in many states across the country, and we have a great deal of experience with contract transitions. Associated with all contracts are dedicated and experienced contract management resources.

Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 56,000 orders in 2014 that were each completed the same day received.

GROWTH & STABILITY – Carahsoft has continued to show impressive growth year after year, turning annual revenue from $3.4 million in our first year in 2004 to $1.065 billion in 2011, $1.465 billion in 2012, $1.8 billion in 2013, and $2.45 billion in 2014. In September of 2014, 7,501 orders were processed worth over $626 million. We are a stable, conservative, and profitable company and have received numerous accolades including the 2013 GovCon Government Contractor of the Year Award in the greater than $300M revenue category. Carahsoft was also recognized in the following areas:

- Largest GSA Schedule 70 Contract holder for software
- 7th of the Washington Business Journal's 100 Largest Private Companies List for 2014
- 2012 Federal 100 Winner, Craig P. Abod, President and CEO
- 2013 Federal 100 Winner, John Lee, Vice President of Cloud Services

As a part of this response Carahsoft has utilized multiple Cloud Solution Vendors, covering all of the Cloud Solution Categories; SaaS, IaaS, PaaS. Carahsoft's strong vendor relationships and partner ecosystem have created an efficient and cost effective response which encompasses all vendor solutions into a single, easy to utilize vehicle. While the technical requirements of each solution vary, Carahsoft strives to consolidate these specifications and responses into a cohesive unit.

MANDATORY MINIMUMS

This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

5.1 – Signature Page

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the Offeror's proposal.

Please find Carahsoft's Signature Page completed above.

5.2 – Cover Letter

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.

5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

Please find above Carahsoft's Cover Letter addressing these requirements.

5.3 – Acknowledgement of Amendments

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

Carahsoft acknowledges all amendments. Also please find below Carahsoft's Acknowledgement of Amendments form completed.

5.4 – Executive Summary

Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

Please find above Carahsoft's Executive Summary addressing these requirements.

5.5 – General Requirements

5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Carahsoft agrees that if awarded a contract they will provide a Usage Report Administrator responsible for quarterly sales reporting described in the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

5.5.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Carahsoft agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading Carahsoft's ordering instructions, if awarded a contract.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

For ease of access and evaluation, Carahsoft has provided these Assessment documents under separate cover. All copies have been submitted electronically per the instructions of the RFP. Please note that specific assessments have been labeled as confidential- additional information is provided in the Confidential, Protected, or Proprietary Information section.

5.5.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

SERVICE LEVEL FRAMEWORK

The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.

Commencement of Service Levels

Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

Service Level Review Meetings

Monthly Service Level review meetings will be conducted by Virtustream with Customer where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a. Promptly investigate and report on the causes of such problem;

b. Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c. Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d. Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e. Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f. Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

a. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);
c. Any hardware, software or other product of a third-party or Customer equipment;
d. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;
e. Downtimes resulting from a Virtustream's scheduled maintenance windows;
f. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;
g. Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;
h. An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a µVM pool that is insufficient to run the designated workload);
i. Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;
j. Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply;
k. Resolution delays due to lack of client response and/or Customer provided credential based information;
l. Priority levels not agreed upon by both customer and supplier;
m. Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

5.7 Recertification of Mandatory Minimums and Technical Specifications

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

Carahsoft acknowledges that if awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in this proposal.

BUSINESS PROFILE

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

6.1 – Business Profile Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.

Carahsoft Technology Corp. was started in Reston, Virginia in 2004. Carahsoft remains headquartered in Reston Virginia employing over 500 people that specifically support the Public Sector (Federal, State, Local, and Public Funded Educational Entities Nationwide within the United States.) Carahsoft has built a reputation as a customer focused organization with depth of experience in government sales, marketing, and contract program management. Carahsoft is one of the largest sellers of Cloud (including SaaS, PaaS, and IaaS) to U.S. the Public Sector.

Carahsoft's organizational structure allows for very focused and individualized support of any customer. The Executive Management team at Carahsoft is responsible for all aspects of day to day running of the organization. Reporting to the Executive Management Team are Directors. It is the Director's primary responsibility to oversee a particular technology area(s) and to monitor and manage all aspects of the staff, customers, and business within that area. An example of a Technology Area at Carahsoft is the VMware Virtualization practice. A host of technology offerings that use VMware at their core are supported by a single business unit overseen by a single Director that has reach back and access to the Executive Management staff. The Director's are then supported by a group of Team Leads. Each Team Lead Oversees a business area (typically defined by customer type (i.e. State Customers) or technology type (i.e. Virtual Desktop). Each team lead oversees a staff that is responsible for executing and managing the activities within that business unit.

At its' core, this organizational structure is lean and efficient, lacking layers of middle management, and empowering individuals with decision making capability in order to support all customers quickly an efficiently.

Carahsoft boasts an excellent employee retention rate. Specific benchmarks that we track include employee retention at 2 years of employment and 4 years of employment with rates of 65% and 90% respectively.

Carahsoft has been providing cloud solutions since opening its doors in 2004. US Public Sector entities have relied on Carahsoft to provide a wide variety of cloud technologies. Carahsoft serves as the cloud distributor and provides access to the core cloud technology with the core technology being supported by companies such as SalesForce, Google, ServiceNow, etc. Carahsoft currently support a state-wide implementation of Service Now's cloud technology within the Commonwealth of Pennsylvania. This implementation is known as the Enterprise Information Help Desk and manages all incident requests. Additionally, in 2013, Carahsoft has contracted with the State of Ohio to provide a cloud solution built around the technology from Salesforce. Ohios' Department of Administrative Services has contracted for Carahsoft to provide a variety of services including Service Cloud, Radian6 and Marketing Cloud as well as others. Both the Ohio and Pennsylvania cloud solutions are still being provided to these organizations.

Contracts similar in scope and size of this NASPO Cloud RFP:

California Multiple Award Schedule	California CMAS 3-12-70-2247E
Delaware Salesforce Contract	Delaware SE-CLD-001
Florida Commercial-off-the-shelf Software Contract	Florida COTS 43230000-14-01
Iowa Salesforce Contract	Iowa 2015-BUS-004
Ohio Master Cloud Services Agreement	Ohio MCSA-0016
Ohio State Term Schedule	Ohio STS 534354
Texas DIR Salesforce Contract	DIR-SDD-1793
Texas DIR Emergency Preparedness Contract	DIR-SDD-2035
Texas DIR Software/SaaS Contract	DIR-TSO-3149
VITA Desktop Productivity Software Contract	VITA VA-140401-CARA

6.2 – Scope of Experience Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred.

CONTRACT VEHICLES – Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Carahsoft holds statewide contracts in many states across the country, and we have a great deal of experience with IT Master contracts accessible to numerous public agencies. Carahsoft has extensive experience in successfully launching, maintaining, and managing these contracts and projects over a wide range of government customers. The range of government projects include agency/ county/ city wide project, state-wide efforts, and multi-state contracts, as well as supporting projects that cross a wide range of Federal government customers. Examples of some of these projects include:

TEXServe Multi-jurisdictional Purchasing Program: Carahsoft promoted and managed the Texserve Contract-allowing the full VMware Products & Services portfolio to be procured by Texas K-12 Users at a discounted price.

> **TEXserve services including**: VMware Technical Support, Pre-sales licensing configuration & design, contract promotion, ad hoc revenue reporting, and customer nurturing/ upsell campaigns. Carahsoft worked with Texserve, K-12 customers, to partner with a select number of VMware Premier and Enterprise Authorized Resellers utilizing their expertise under the Texserve contract.

ONENET Purchasing Consolidation: Carahsoft serves as the prime contractor and program manager for the ONENET contract serving the entire ONENET community providing the ability to procure VMware software (licensing/support) through a trusted network of strategic partners at a discounted rate. Carahsoft has a proven track record of providing the highest level of technical support while ensuring that members receive the proper software products and services conveniently under the ONENET Contract.

TX DIR Contract Sales: Carahsoft maintains a number of purchasing vehicles with the State of Texas Department of Information Resources (DIR.) 2014 DIR sales accounted for greater than $50M in revenues. Carahsoft actively markets these contracts and has grown revenues at greater than 10% annually for the past 5 years.

Total GSA State & Local Sales: Carahsoft holds a US General Services Administration (GSA) Schedule 70 Technology Contract. This contract is open to State and Local agencies to purchase as a form of Cooperative

Purchasing. Carahsoft markets the availability of this contract to eligible users and maintains sales revenues to eligible State and Local entities at greater than $50M annually.

As a whole, Carahsoft's five largest public sector contracts have totaled approximately $211,571,007 in sales in the past 2 years.

Carahsoft GSA Schedule	GS-35F-0119Y	$127,242,948.95
Texas DIR Emergency Preparedness Contract	TX-DIR-SDD-2035	$ 39,007,058.19
Texas DIR BMC Contract	TXDIR-SDD-1727	$ 15,734,306.68
Texas DIR Salesforce Contract	TXDIR-SDD-1793	$ 14,876,679.26
Texas DIR Adobe Contract	TX-DIR-SDD-2504	$ 14,710,013.43

Total Sales: $211,571,006.51

These contracts make up close to 2/3 of the total sales on contract that Carahsoft completed in that span. All of these contracts are currently in place with government entities.

6.3 – Financials Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Carahsoft has deemed its audited financials to be considered confidential. Additional information is provided in the Confidential, Protected, or Proprietary Information section. For D&B report along with additional clarification, please see page 360 in the Supplemental Information Section.

6.4 – General Information

6.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

Carahsoft has assembled a team from our vast portfolio of vendors that includes our leading premiere network of cloud solutions, resellers, and subcontractors as the best solution to meet the State of Utah's requirements. They include:

AODocs, CA, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, Virtustream, VMware

Carahsoft is submitting as the exclusive offeror for all Google, Salesforce, and ServiceNow solutions and services for the NASPO Cloud solicitation. These manufacturers have deemed Carahsoft as the prime contractor who can effectively and efficiently manage the NASPO cloud contract on their behalf.

As a part of this response Carahsoft has utilized multiple Cloud Solution Vendors, covering all of the Cloud delivery models; SaaS, IaaS, PaaS. Carahsoft's strong vendor relationships and partner ecosystem have created an efficient and cost effective response which encompasses all vendor solutions into a single, easy

to utilize vehicle. While the technical requirements of each solution vary, Carahsoft strives to consolidate these specifications and responses into a cohesive unit. For example:

CA Technologies is a leader in IT Management Solutions in the industry. CA has be steadily moving its premier on premise management solutions to the cloud. CA Clarity Project and Portfolio Management (PPM) is one of the leading solutions used by state governments today.

Google's SaaS offering, Google Apps, has been commercially available since 2006 and presently has ~5.3 million paying customers covering 26m+ end user licenses. Google Apps represents a combination of the most popular consumer products that have been prepared for Enterprise use through the means of adding Administrative and Compliance Controls to the suite.

Gmail is the anchor product in the SaaS offering. Google has over 1B consumer users of Gmail and from that success designed a means by which customers could bring their own email-enabled domain name(s) into this managed service to replace legacy on-premises systems at a significantly reduced price. The straightforward means of migrating data as well as configuring the service and the knowledge that a majority of these business users may already be familiar with Gmail via personal use has made the adoption of Google Apps a logical choice.

Examples of the evolution of this SaaS offering include:
● Acquisition in 2007 of one of the leading email security and compliance vendors and the integration of those services to the Gmail Advanced Settings options. These features include the ability for customer System Administrators to set Spam, Content, Attachment and TLS policies to meet their specific requirements.
● In 2011 Google launches the Google Apps Status Dashboard, a publicly accessible website with RSS feeds to keep the world apprise of current system status.
● In 2012 Google increases the Gmail storage allocation from 10gb to 25gb, no change in price
● In 2013 Google modifies the storage space to unify email and Drive storage and increase the allocation to 30Gb, no change in price
● In 2014 Google offers a new premium SKU that offers unlimited unified Storage
● In 2015 Google enhances the Gmail Advanced Settings features to include pre-defined lexicons to support Data Loss Prevention scanning in email.

The above list is a short list of the variety of services, support offerings, features and best practices that Google has adopted into the service delivery of the SaaS offering. In addition to the wide use of GMail, Google has six other products with over a Billion active users. Those are Google Search, Chrome, Android, Google Maps, YouTube and Google Play.

Chrome as a browser and an operating system are further evidence of strong usage and market acceptance. In a report released by Net Applications in April of 2015, Chrome browser held 25.68% market share while IE11 had 25.04, followed by IE8 at 16.0. The increase in adoption by Enterprise customers is attributed to the real time updates against emerging threats and the Chrome for Enterprise browser controls.

Chromebooks, the laptops that run Google Chrome as the OS, are seeing a rapid increase in sales in the K-12 market worldwide. This is attributed to the low-cost and the easy-to-manage machines.

Google's PaaS/IaaS offerings entitled Google Cloud Platform was first announces in 2008 with Google App Engine, a platform to develop and host web applications. Early success on this platform included The Royal Wedding Website and BestBuy moving their online Gift Card/Registry service to the platform. Over the years, and based on market demand, Google began to externalize off PaaS/IaaS service offerings that Google developed originally for their own infrastructure and platform utilization.

Google continues to expose the benefits of Google's infrastructure to outside entities.

Or, put differently, Google lets customers use the same infrastructure that allows Google to return billions of search results in milliseconds, serve 6 billion hours of YouTube video per month and provide storage for 1Billion Gmail users.

Salesforce is the enterprise cloud computing leader dedicated to helping companies and government agencies transform into connected organizations through social and mobile technologies. Since launching its first service in 2000, Salesforce's list of over 150,000 customers span nearly every industry worldwide. The company's trusted cloud platform is creating a connected government experience for over 1000 government agencies including all federal cabinet government agencies and the majority of US States. With the world's leading cloud platform, Salesforce is freeing government data from legacy systems, empowering citizens and connecting agencies to administer government in powerful new ways. Government agencies are using Salesforce solutions for a multitude of government functions including grants management, constituent communications and correspondence management, incident and case management, call/contact center management, outreach programs, learning management, volunteer management, project management, and even donor management, among numerous others.

SAP is the fastest growing company at scale in the cloud with a user base of over 95 million subscribers. We also have the largest cloud portfolio of over 30 solutions for all lines of business as well as business suites. We also have 41 data centers in 21 locations in 11 countries.

6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, our various cloud providers continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Some examples include:

ServiceNow's security framework is based on ISO/IEC 27002 and has been ISO 27001 certified since 2012. Annually, ServiceNow undergoes ISO 27001 Surveillance audits and well as SSAE 16 attestations for both SOC 1 Type 2 and SOC 2 Type 2. Customers under an NDA can request these reports annually in assisting with both their vendor management and regulatory or compliance programs. ServiceNow provides Security Event Logs using Application Level Audit Logs and Infrastructure Monitoring,

Application Level Audit Logs. The ServiceNow application writes detailed audit log information that is stored in tables within a customer's instance. Since this is considered customer data and is stored within a customer's instance, ServiceNow does not attempt to monitor or view this data unless specifically requested by a customer. As a result the customer is responsible for monitoring the contents of these logs files and, at the customer's choosing, exporting the logs through the capabilities provided within the platform.

Infrastructure Monitoring. All components of the infrastructure supporting the private cloud feed alerts and logs into the SIEM. In addition, ServiceNow has deployed an Intrusion Detection System (IDS), positioned to listen to all inbound network traffic, with all events going to the SIEM as well. The SIEM is configured to automatically send alerts for common attacks. ServiceNow is responsible for managing the SIEM environment and securing the logs. ServiceNow retains all infrastructure logs for at least 90 days. The Security Operations Center (SOC) is also responsible for completing a daily checklist across a range of security domains, including privilege account usage, IDS alerts, file integrity monitoring (FIM), and database access. The daily checklists and captured events are managed through an instance of ServiceNow. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.

CA SaaS environment is compliant with SSAE16 for services where infrastructure and application are managed and maintained by CA. CA Agile Management currently does not hold SSAE16 certification. For SaaS offerings where infrastructure is managed by a third party, provider's SSAE16 reports are available upon request.

6.5 – Billing and Pricing Practices

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

Carahsoft's Order Management team works to ensure that billing and payment are completed in an efficient and simple manner. Purchase Orders and Invoices are provided to the customer early to ensure that payment can be completed whenever the customer is ready and within the confines of the agreed upon deal. Our OM team is available to answer any questions a Purchasing Entity has in order to assist with the process and confirm that they have everything needed for payment.

Carahsoft's pricing is dictated by the manufacturers- Carahsoft ensures that the Purchasing Entity's receive the best possible price by working directly with the manufacturer and ensuring that pricing meets or exceeds the contract being used. In addition, Carahsoft works with the manufacturer to ensure that all pricing changes are accounted for within the contract, as applicable.

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

When a purchasing entity determines they need implementation services to their cloud solutions, the Carahsoft offering provides these additional services. For Example:

ServiceNow Response: Customers typically engage ServiceNow for the initial implementation and training services and then for any major new future application implementations to get the best-of-breed expertise

for good standard solution support. ServiceNow developed the platform and applications so anyone could support changes to the configuration without having to hire outside consultants. The customer is empowered as they gain experience either by shadowing ServiceNow consultants during initial implementations, as they talking to other customers through the Community website, or by asking for technical support through the portal. So initial costs typically occur for ServiceNow when it is first implemented and there might be requested services as customers add new application support but there are no ongoing costs typically.

CA Cloud SaaS solutions are fully operational multi-tenant solution that are fully ready to use at outset. These Solutions are typically complex management solutions that do require setup and training. For example many customer will purchase a limited time block of consulting to help with loading data, and configuring reports. Training is also available for all applications to either augment start-up packs or walk customers through basic tasks.

In addition to the licensing fees there are optional Google services that a Purchasing Entity may find meet additional mandatory requirements. Examples would include adding on other SaaS solutions like Virtru for end to end encryption or AODocs for Document Management. The key benefit to moving to Cloud based vendors is a new set of transformative tools that are more productive and most cost effective than traditional client server solutions. Other additional costs may come into play of the Purchasing Entity wants to outsource all of the configuration and migration work to the selected reseller leading to additional time and materials expenses.

The Salesforce solution is available immediately for use via the internet after a Purchasing Entity makes a purchase of the solution. Other additional costs would include any implementation fees to be performed by a certified Salesforce implementation partner. These fees vary based on the type of project and length and complexity of implementation.

6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

Carahsoft's cloud solution offerings all fit within the guidelines listed in NIST publication 800-145 and repeated in Attachment D of this response. Please see response 8.1.5 for a more detailed explanation.

6.6 – Scope and Variety of Cloud Solutions

6.6 Specify the scope and variety of the service models you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer.

Carahsoft proudly offers a number of SaaS, PaaS, and IaaS supported by the cloud technologies as listed below. Many of our top tier cloud vendors also provide subscription and utility based pricing models which would be available to the State. Below is a list of each manufacturer being proposed in this response, along with the specific type of solution (SaaS, IaaS, and PaaS) they fit into:

SaaS – AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
PaaS – Google, QTS, Salesforce, SAP, ServiceNow, Virtustream
IaaS – FireEye, Google, QTS, Virtustream, VMware

6.7 – Best Practices

6.7 Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Carahsoft utilizes varying procedures for ensuring visibility, compliance, data security and threat protection for cloud-delivered services. Please see the below examples of potential options for meeting the State's expectations:

ServiceNow Response: ServiceNow applications have the advantage of being built on a single cloud platform that consists of one user interface, one code base and one data model; delivering holistic visibility into processes, creating a single source of truth, irrespective of whether the processes and systems are within the customer's environment or hosted in the cloud. ServiceNow invests significant resources in providing its services in a secure manner. This includes global teams delivering 24x7 operations and technical support from ServiceNow staff. ServiceNow currently has offices with staff focused on the management of the private cloud in Australia, the Netherlands, the U.K, North America, and Asia. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow, which supports a logically single tenant architecture. Customer data is isolated from other customer data by leveraging an enterprise-grade cloud architecture and a dedicated database and application set per instance. This gives ServiceNow customers cost reduction through shared infrastructure, while having the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each customer instance, customers can leverage the additional security features within ServiceNow to augment the security configuration of their instances based on their own needs and risk profile.

CA Response: This is addressed throughout all of our policies and procedures. CA SaaS Operations and Delivery runs an Information Security Management Framework (ISMS), which includes security organization, documentation, monitoring, and continuous improvement cycle. The security documentation comprises of CA SaaS Operations information security policies, procedures, guidelines and checklists. ISMS documentation is reviewed along with applicable controls annually. CA offers a variety of SaaS solutions, details for each offering has been provided in Exhibit 1 and 2 of this proposal.

Salesforce Response: Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements. Encryption options vary based on Salesforce Commercial Cloud or Salesforce Government Cloud offering.

Government Cloud Encryption:
As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2 cryptographic implementations for data being transferred between the State's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below.

Data In Motion:

Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048- bit Public Key. Our service uses International/Global Step Up certificates. We support one- way TLS, in which customers create secure connections before sharing private data.
Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary.

Data At Rest:
NIST SP 800-53 Rev. 4 states in SC-28, “Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.” SC-28 also states, “Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.” All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce’s secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data.

ORGANIZATIONS PROFILE

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

7.1 – Contract Manager

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have a minimum of three (3) years' experience managing contracts for cloud solutions.

7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Bethany Blackwell
Senior Manager
703-230-7435 (office)
703-501-1134 (cell)
Bethany.blackwell@carahsoft.com
Working hours: 7am-7pm EST M-F

7.1.2 Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

The proposed contract manager, Bethany Blackwell, has over 5 years of experience in managing SaaS contracts in both the State and Local and Federal markets.

Bethany developed and manages contracts and associated terms for cloud contracts in more than 10 states. The combination of the State and Federal contract vehicles and BPAs being managed is valued at over $300M. Annually, she oversees 1000+ SaaS transactions off of these contract vehicles which include licensing and implementation that provide end to end cloud solutions to public sector customers.

Name	Position
Bethany Blackwell	**Carahsoft Senior Account Manager – Will serve as the NASPO ValuePoint Contract Manager**
Background	
• Senior Manager for cloud solutions products, including Salesforce.com, DocuSign, BMC Software • Vendor/Partner manager for 20+ complimentary solution vendors and 25+ implementation partners and system integrators • Graduated Virginia Tech in 2010 - dual degree with concentrations in Psychology and Political Science • 5+ years of experience at Carahsoft	
Skills	

• Expertise in negotiating SaaS contract vehicles and terms at State level • Knowledge of contract vehicles, BPAs, multi-year deals, multi-vendor deals • Management of enterprise size product contracts • Establish and maintain positive customer relationships through proactive communication • Maintained interactions with customers to ensure quick, accurate quotes; facilitated easy ordering process for customers
Relevant Experience
• Oversees the management and execution of 900+ individual SaaS contracts, valued at 85M+ annually • Maintain the annual recurring subscription renewal bases to ensure no customer's lapse in service • Oversees the ordering and distribution of licenses on statewide enterprise licenses agreements and various BPAs • Established vendor specific terms and conditions for 10 different statewide contracts • Assist customers in shifting buying strategy from perpetual to subscription licensing model

7.1.3 Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

The Contract Manager assigned to this contract will be in charge of all coordination and organization efforts between Carahsoft and NASPO ValuePoint. This includes, but is not limited to:

- contract negotiation
- roll-out plan
- amendments completion
- renewal execution
- reseller/subcontractor additions
- contract pricelist updates and upkeep
- contract compliance
- marketing coordination

TECHNICAL RESPONSE

This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

In response to the State of Utah request for Cloud Solution Proposals, Carahsoft has assembled a response that includes a number of Cloud Solution Offerings from within the Carahsoft Cloud framework. These offerings are all supported in part or wholly by twelve leading cloud technology providers. Each provider's technology is an integral part of Carahsoft's proposal. Within this framework, Carahsoft will orchestrate, assemble, and execute on all activities necessary to support this contract, engaging each cloud technology provider as needed in the delivery of a particular service or solution offering.

The Carahsoft Cloud framework will provide for all requirements of the State of Utah Request for Proposal to be fulfilled. Carahsoft will be able to provide Cloud Solution Offerings to the State of Utah as well as to those entities that may participate via the cooperative purchasing program. The Carahsoft Cloud proposal provides for the provision of PaaS, IaaS, and SaaS offerings that are compliant with all requirements as outlined by the State. Carahsoft will provide dedicated resources to supporting this agreement. Carahsoft will insure that adequate resources are supplied to fully support this agreement during all phases from contract launch through termination. Usage requirements and demand resources fluctuate over time and Carahsoft's Cloud offering has been constructed in a manner that provides for the ability to scale without interruption, disruption, or any other similar interruption of customer service and solution availability.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

For the purposes of Carahsoft's response to the technical requirements (section 8) of this RFP, please note that any response provided related to a specific manufacturer should be treated as a response to the following categories:

SaaS – AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
PaaS – Google, QTS, Salesforce, SAP, ServiceNow, Virtustream
IaaS – FireEye, Google, QTS, Virtustream, VMware

8.1 – Technical Requirements

8.1.1 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

CA	APM	CA APIM SaaS offering helps accelerate, secure and manage APIs. CA is responsible for development and management of application. AWS provides IaaS services to CA for management of the underlying cloud infrastructure.
	MAA	CA Mobile App Analytics stimulates collaboration between business analysts, developers, operations and support in order to accelerate mobile app delivery and improve end-user experience. This service is hosted at CenturyLink Data center and the infrastructure is managed and maintained by CA SaaS Ops and Delivery team.
	CA Agile	CA Agile Central is a SaaS offering that is generally used to document and manage work within the SDLC.
	ASM	CA App Synthetic Monitor (ASM) provides end-to-end transaction response-time visibility into cloud, mobile and Web applications. Application utilizes Rack Space IaaS services.
Google	The Cloud Service Models that we intend to provide include SaaS, PaaS, and IaaS. In our response we will describe the various options for using Google Apps under the SaaS model and the functions of Google Cloud Platform under Paas and Iaas.	
AODocs	The Cloud Service Models that we intend to provide is SaaS.	
Virtru	All Virtru services are cloud-based and accessed via browser or downloadable browser extensions and plugins.	
Salesforce	Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145	
ServiceNow	Cloud service model: Software as a Service (SaaS) Deployment model: Private Cloud	
QTS	"QTS is a leading national provider of Infrastructure as a Service (IaaS) data center solutions and fully managed cloud services and a leader in security and compliance. The company offers a complete, unique portfolio of core data center products, including custom data center (C1), colocation (C2) and cloud and managed services (C3), providing the flexibility, scale and security needed to support the rapidly evolving hybrid infrastructure demands of web and IT applications. With 12 data centers in eight states, QTS owns, operates and manages approximately 4.7 million square feet of secure, state-of-the-art data center infrastructure and supports more than 850 customers. QTS' Critical Facility Management (CFM) can provide increased efficiency and greater performance for third-party data center owners and operators. QTS offers a number of IaaS solutions.	
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	The SAP Fieldglass application is exclusively offered in a software as a service (SaaS) model.
	Hanna	SAP HANA Enterprise Cloud (HEC) is a private managed isolated & dedicated ladnscape (single tenant) offering end-to-end cloud-based infrastructure and managed services for SAP applications powered by SAP HANA. It is a fully scalable, enterprise-ready, mission-critical, secure and high-availability cloud service.
	Hybris	The SAP Hybris Commerce, Cloud Edition offering are all single tenent hosted VM environments. Customers have their own VM's with SAP Hybris instances deployed to those VM's. The SAP Hybris Commerce, Cloud Edition currently

		has Development, Staging, Testing, and Production environment. More environments can be added as required.
	SuccessFactors	Our solutions are delivered through a private cloud using a multi-tenant architecture. We refer to this as a Controlled Cloud. It includes a contractual framework reflecting applicable data privacy regulations, implementation and maintenance in accordance with Technical and Organizational Measures (TOMS) and regular audits by an independent third party for industry compliance and transparency.
VMware	vCloud Air	IaaS – Public, Hybrid, Community
	Horizon Air Desktop & Apps	IaaS – Public
	vCloud Suite	IaaS – Private, Hybrid, Community
	Airwatch	IaaS – Private SaaS – Public
	Horizon 6	IaaS – Private
	Realize Air Complaince	SaaS – Public
	SocialCast	SaaS – Public
FireEye	All FireEye cloud offerings included in this response fit the SaaS cloud service model and private cloud deployment model.	
VirtueStream	Virtustream solution is fully NIST compliant for Essential Characteristics, as the Infrastructure as a Service (IaaS) Service Model, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud.	

8.1.2 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following characteristics, as defined in NIST Special Publication 800-145:
8.1.2.1 NIST Characteristic – On Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

CA	APM	N/A. This is a SaaS service and clients do not have direct access to the underlying infrastructure in order to provision computing capabilities. CA is responsible for the management and maintenance of the infrastructure and will make any necessary adjustments as part of providing this service to its clients.
	MAA	This is a SaaS offering and On-Demand service is not available, however, MAA customers are enabled to manage their accounts and carry out configuration changes required to manage mobile applications.
	CA Agile	We are a fully multi-tenant environment and do not provide the On-Demand Self-Service capability.
	ASM	This does not apply as this is a SaaS service. ASM customers are able to manage all aspects of their accounts, create sub-accounts, and make any configuration changes necessary for their monitors.
Google	SaaS, Google Apps administrators have access to an Admin Panel that allows them to perform user administration, service configurations, reporting on demand. Paas/IaaS, Google Cloud Platform is an integrated set of Compute tools, Storage Tools, Networking Tools, Big Data analytic tools, Management tools and Services APIs. A customer can use any of these services on demand via the Developer's Console.	
AODocs	SaaS, AODocs administrators have access to an Admin Panel that allows them to perform user administration, product configurations,reporting on demand.	

Virtru	All required services can be provisioned immediately when required. Users only need to install application to get single-user capability, or login to administrative dashboard for administrative features.	
Salesforce	Salesforce PaaS and SaaS solutions are delivered on-demand via the web and can be accessed with a browser and internet connection or mobile device. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up customers to manage their mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE). No installations on users' laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.	
ServiceNow	Customer instances are provisioned automatically after an agreement between a customer and ServiceNow is executed. ServiceNow actively monitors customer instance performance and can automatically scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.	
Docusign	DocuSign's DTM® solution is ISO 27001:2013 certified and many of the ISO 27001:2013 controls are mapped to the NIST 800-53 requirements; we can provide additional information upon request.	
QTS	On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.	
SAP	Ariba	The solution provides self-service user profile management. Users profit from the intuitive, minimal-step nature of the user interface with little or no training. Changes to user profile includes workflow capability for profile changes.
	Fieldglass	All system resources are available to all customers without limitation. The system is highly configurable with most configurations being available to the customer's administrators.
	Hanna	HANA Enterprise Cloud is a private managed cloud therefore infra & services could be requested (added or decommisioned) on demand by placing change requests with SAP HEC teams. HEC roles & responsibilties document clearly articulates what is included in the monthly HEC pricing and what is available on-demand in addition to scaling up or down on the infra/compute.
	Hybris	N/A
	SuccessFactors	All self-service is in one place, including benefits and payroll if those products are in scope. Self-service is an intuitive experience. We provide the ability for employees to have configured permissions to take action in the tool such as field or data updates for personal information, benefits changes, payroll actions, completing workflow for assigned activities in the tool, etc. Self-service for both employees and managers is configurable to fit your business rules and organizational requirements.
VMware	VMware's IaaS and SaaS offerings complies with the On-Demand Self-Service characteristic, because once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. The subscription includes access to two self service consoles: My VMware for account management, and the VMware vCloud Air Console which is the primary interface for access consumption and management of cloud resources purchased from VMware. (See doc for a complete list of products/ features that comply)	
FireEye	FireEye is offering 4 distinct SaaS cloud solutions each featuring self-service features specific to the unique capabilities of the offerings: 1.Email Threat Prevention (ETP) Email Provisioning	

	Once the ETP infrastructure is provisioned, customers can self-service the acceptance of up-stream mail and delivery to user mailboxes by configuring their own domain settings. No user mailbox provisioning is required as ETP will automatically check the validity of the email recipient with the downstream service. 2.Mobile Threat Prevention (MTP) User Provisioning Once the MTP infrastructure is provisioned, customers can self-service the creation of service users by integrating with an LDAP service or manually adding the users via the user interface. Device Provisioning Once the MTP infrastructure is provisioned, customers can self-service the creation of managed devices by instructing users to install the FireEye MTP Application on their mobile device and having a valid user account provisioned. 3.Threat Analytics Platform (TAP) User Provisioning Once the TAP infrastructure is provisioned, customers can create and assign role-based access control to user accounts. The enrollment process includes the ability to create two-factor authentication for newly provisioned users. Data Sources Once the TAP infrastructure is provisioned, customers can configure new data sources to feed the TAP instance without the assistance of FireEye. The TAP communications broker accepts data feeds in the following formats: syslog, flat files, TCP/UDP streams, and JDBC connections. 4.FireEye as a Service with Continuous Vigilance (FaaS CV) User Provisioning Once the FaaS infrastructure is provisioned, customers can create and assign role-based access control to user accounts via the on premise FireEye sensors.
VirtueStream	Virtustream IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP. Virtustream portal that enables the user to provision VMs, order services through a catalog, add storage, upload service templates, and run various reports all through the same portal.

8.1.2.2 NIST Characteristic – Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

CA	APM	The APIM service is accessed via HTTPS on a supported browser with no requirements for a workstation client install ; mobile friendly and optimized for use with iOS and Android tablets
	MAA	Upon native authentication, MAA dashboard is accessible by any host over public internet. Also, mobile devices connect to the service using REST API.
	CA Agile	All access to the application is through a browser.
	ASM	The ASM dashboard and API are accessible from any host connected to the public Internet. The API and dashboard require authentication, and each account is only accessible by the account owner (customer).
Google	SaaS, Google Apps is device, platform and network agnostic. As a pure play cloud-based solution the services can be accessed via any modern browser from any network access point. Customers that have requirements to limit access to trusted devices or trusted access points have access to Device Management tools via the Admin Panel at no additional cost. PaaS/IaaS, Google Cloud Platform management services can be accessed via any modern browser from any network access point. End-users can accesses services through one or more	

	appropriate tools (browser, CLI, APIs, etc.). Administrators can also monitor and manage services through a mobile app.
AODocs	SaaS, AODocs is service, platform and network agnostic. As a pure play cloud-based solution the services can be accessed via any modern browser from any network access point.
Virtru	All Virtru services are available on the publically available internet.
Salesforce	Salesforce PaaS and SaaS solutions are delivered on-demand via the web and can be accessed with a browser and internet connection or mobile device. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up customers to manage their mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE). No installations on users' laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.
ServiceNow	ServiceNow's physical architecture is deployed into ServiceNow's managed dedicated colocation cage space. Multiple diverse Internet connections terminate within the dedicated cage space providing redundant access from the Internet to the ServiceNow environment. All users, administrators and developers connect to the ServiceNow private cloud over HTTPS, leveraging TLS, for communication to and from a ServiceNow instance with all normal interactions via a web browser. There is no requirement to install any client software on any desktop, laptop, tablet, or smart phone used to access a ServiceNow instance.
Docusign	Please see above.
QTS	Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). QTS recognizes that the connectivity challenges of today are largely driven by consolidation, virtualization and adaptive architectures. Our agile connectivity solutions provide you with both unification across your communication infrastructure and with built-in network scale, reliability, and high-performance. QTS metroConnect is a fast, reliable, high bandwidth connection to hundreds of network and service providers inside the local Carrier Hotel. With access to the numerous networks at the carrier hotel, QTS delivers the interconnection necessary to support your connectivity, business continuity and application collaboration needs. metroConnect offers redundancy and diversity options that ensure your content is always available. •High availability •Backed by a 99.999% SLA •24x7x365 monitoring and management •Carrier-neutral model •Convenient access to an array of Carriers and Internet providers •Dedicated, secure, and highly resilient connectivity with speeds of 100Mbps, 1Gbps or 10Gbps* •Supports all connectivity redundancy, business continuity, and collaborative application needs QTS data centerConnect Service Data centerConnect is a secure, scalable, cost-effective way to connect your primary and secondary sites between two or more client environments located in different QTS data centers providing a reliable interconnection option for any size business. QTS data centerConnect enables data replication and recovery through its resilient and redundant network. This ensures your business operates successfully with seamless, day-to-day transactions over a high-performance, low latency connection that supports business continuity, data replication and other IT business application needs. With QTS data centerConnect you get: •High Availability – Resilient network architecture provides high availability and reliability

	•Dedicated and Secure – Dedicated bandwidth with secure MPLS encapsulation •Scalable Bandwidth – Easily scale your bandwidth (from 10Mb up to 1Gb) •Flexible Network Configurations – Supports multiple network topologies •Cost-effective, Bundled Solution – All inclusive, bundled offer •Fully Managed, End-to-End – End-to-end, proactive monitoring and management, 24x7x365 QTS internetConnect Service internetConnect provides a multi-homed, high performance, dual access, multi-carrier network that meets all your Internet service needs. We ensure maximum uptime, guaranteed availability, and various bandwidth speeds through our flexible, high performance, carrier-neutral offer. For enterprises and government agencies conducting business over the Internet, QTS internetConnect Service provides a highly reliable, secure connectivity solution for production environments. •Direct access to multiple ISP backbones gives unmatched reliability and guarantees maximum uptime ◦Dual connections with direct access to multiple ISP backbones ◦Diverse, redundant paths to multiple backbone providers ◦Dual paths, with diverse entry points into the QTS Data Center •Anti-DDoS Mitigation Services provide an additional level of protection and security •Dedicated with burstable bandwidth options provides resiliency and flexibility •Backed by an industry leading 100% SLA •Optional service plans to meet your needs QTS ethernetConnect Service You need to be able to connect your employees and customers to your applications and to the outside world. Whether hybrid cloud, disaster recovery/disaster recovery as a service, data replication, data migration or other applications, you need the ability to seamlessly and conveniently connect your business together and to the outside world as if there is no distance between you. QTS ethernetConnect offers a variety of connectivity options. You can centralize your services with a single provider. And since QTS can handle everything from ordering to billing you have a single provider for a complete solution – “One Stop Shopping”. QTS understands your needs and will tailor your end-to-end solution for your business. •High Bandwidth – Speeds are available in select increments of 100Mb to 10Gb •Data Privacy – Data is separated from IP traffic as it traverses the carrier backbone •High Performance Options – Solutions can be developed to fit your specific performance or reliability requirements •Consistency – Ethernet circuits travel over a single carrier’s infrastructure and data follows a consistent path.
SAP	Ariba	Ariba uses Cisco Routers and Catalysts (high-speed switches) for ensuring maximum network connection performance. They deliver enterprise-class versatility, integration, and power to Ariba. Together, these routers provide the required support for Internet/intranet access with firewall security.
	Fieldglass	Customers are only required to use a standard web browser with default settings to access and use the Fieldglass solution.
	Hanna	Cloud Capabilities are available over the network (via secure MPLS or VPN network connectivity) and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops. HEC is an extension of customers existing netwerk and uses customes IP range and /24 range.
	Hybris	All capabilities of SAP Hybris are available over the network. Furthermore, they are accessible by standard mechanism including heterogenous thin or

		thick client platforms through either standard web technologies or through the hybris OCC REST web service API's.
	SuccessFactors	Our solution was designed from the outset for high availability. We provide a system availability SLA of 99.5%. Every component (hardware and software) is completely redundant. There is a redundant piece of equipment or software for every hardware or software component for every layer of the infrastructure stack (server, software and network). We load balance at every tier in the infrastructure, from the network to the database servers. F5 load balancers are used to route traffic to an available web server to process the request. Application server clusters are enabled so that servers can fail without interrupting the user experience. We maintain an N+1 approach for all equipment in the hosted cloud environment, so that there is never a single point of failure. All customer database backups are encrypted and streamed in a secure manner from the customer's "primary" data center to their "alternate" data center, allowing for a timely restoration of service in the event of disaster. Based on the terms of the agreement, we will designate one of the data centers as the customer's "primary" data center, with an additional data center designated as the "alternate" for data redundancy and disaster recovery purposes. Load balancers will automatically detect a software or hardware error and take the servers out of service if needed without interrupting the user experience or application. They also allow capacity addition or reduction without interrupting service. All of the JBOSS application servers are clustered. Each is designated as a primary and a secondary, so any application server can fail without any loss of service or interruption of the application or user experience. The database servers are also clustered using a Veritas high availability cluster. The Veritas suite will detect any hardware or software errors in the database machines and automatically fail them over to a standby server
VMware	VMware's IaaS offerings complies with the Broad Network Access characteristic. All fo these products' capabilities are available over the public internet and can be used by heterogeneous thin or thick client platforms. Consumers only need internet access to access these resources. Additional capabilities exist including the ability to secure communications over the public internet including IPSEC VPN, SSL Client VPN, and the ability to consume via WAN connectivity. VMware's SaaS offering AirWatch can be accessed over the internet or private network through standard mechanisms.	
FireEye	All FireEye cloud offerings included in this response meet the definition of broad network access. Each of the solutions performs its designed functionality over standard internet-facing services and is accessible via a web browser from any internet connected device when valid credentials are provided.	
VirtueStream	Virtustream IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, etc.) which is growing rapidly as option for connecting cloud resources.	

8.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

Carahsoft's multiple Cloud Service Provider's solution provides for Resource Pooling, as defined by NIST, in a variety of methods. Each method optimizes the cloud subscriber's experience while optimizing the availability of compute, network, and data resources. Each service provider provides Resource Pooling, see below for details.

CA	APM	CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon's infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.
	MAA	MAA core service utilizes dedicated infrastructure layered with virtualization capabilities. It doesn't share computing resources with other services. Tenants are segregated using application containerization capabilities.
	CA Agile	We monitor all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. We can easily scale our systems to accommodate any additional capacity. If we determine a single user is using a significant amount of resources we will proactively reach out to them to understand what they are trying to accomplish and help them to formulate more performant queries.
	ASM	All ASM core servers are dedicated physical servers. ASM Public Status Pages are served from dedicated web servers (used only by CA ASM) in the Amazon Cloud, on shared tenancy virtualization. Amazon Cloud virtual machines used by ASM are managed by and provisioned by CA ASM systems administrators.
Google	SaaS, Google's global infrastructure is a shared pool of resources that dynamically serve each end user with a primary data center access point that may rotate throughout the session without the end user being aware while at the same time replicating any data across at least two additional geographically dispersed data centers which also may rotate through the session. PaaS/IaaS, Google Cloud Platform also operates across the global Google infrastruture. The elements of this service can be defined within the Developer's console to run within a higher level of abstraction which covers four regions; Central US, Eastern US, Western Europe, East Asia where each region has three or four zones.	
AODocs	AODocs infrastructure is hosted in Google App Engine and data of our customers on Google Drive. This protection is insured by Google.	
Virtru	Virtru Services are offered in a fully multi-tenant mode if the customer requests.	
Salesforce	Salesforce is a multitenant cloud-based subscription service. Multi-tenant cloud solutions provide a single, shared infrastructure, one code base, one platform that is all centrally managed, with platform-based API to support all integration traffic, and multiple release upgrades included as part of the subscription service. Multi-tenancy and the Cloud Computing model remove unneeded tasks from the process of delivering, managing, and integrating software. Salesforce customers will not need to maintain any hardware or software. Without multiple versions to support, integrations don't break during updates; they are simply updated automatically. As a result, both the initial integration and its continued maintenance are simplified. More resources can be focused on creating a better product, with a faster cycle of innovation, instead of having to manage the complexity of many different versions to support a vast installed base. Salesforce's position as an online service enables us to roll out all levels of improvement, from patch releases to major upgrades that are largely transparent to the end users. When a bug is fixed and tested, it is rolled out to the application as part of regular maintenance; the nature of the service prevents special patches and code branches for individual customers, so all fixes can potentially benefit all customers.	
ServiceNow	The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow, which supports a logically single tenant architecture. Customer data is isolated from other customer data	

	by leveraging an enterprise-grade cloud architecture and a dedicated database and application set per instance. This gives ServiceNow customers cost reduction through shared infrastructure, while having the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each customer instance, customers can leverage the additional security features within ServiceNow to augment the security configuration of their instances based on their own needs and risk profile. Customers share a hardware platform (no virtualization), but access entirely separate individual instances of the ServiceNow platform.	
Docusign		
QTS	Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.	
SAP	Ariba	Ariba recognizes that customers need the highest-possible availability and reliability. To that end, Ariba infrastructure is scalable and redundant at all tiers. To provide high availability and reliability, Ariba has extensive error handling and fail-over capabilities. In order to ensure the highest availability, Ariba uses such best practices as frequent systems backup and maintenance, redundant systems, proactive customer notification of unplanned down-time and international support coverage.
	Fieldglass	Fieldglass is offered in a SaaS model. All customers access the same Fieldglass application version in a multi-tenancy database. The system is hosted in a secure hosting facility. All system resources are available to all customers without limitation.
	Hanna	SAP HEC does not pool resources for critical business systems as it's a managed private cloud, which is dedicated to one particular customer. However, network routers, availability reporting & monitoring could be shared. Details can be provided during HEC technical assessment workshop.
	Hybris	All computing resources of the data centers are pooled to serve multiple customers. Each customer gets their own separate VM's and their own instances of hybris deployed to those VM's.
	SuccessFactors	Load Balancing & Server Clustering – We load balance at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled so that servers can fail without interrupting the user experience. Database servers are clustered for failover. We maintain an N+1 approach for all equipment in its hosted environment, so that there is never a single point of failure. Complete Redundancy - Every infrastructure component is redundant. There are at least two of each hardware component that processes the flow and storage of data. Backup & Restore - the Data center runs full data backups weekly and incremental data backups nightly.
VMware	All VMware's IaaS products comply with the Resource Pooling characteristic (except for the Hybrid Cloud Manager which is Not Applicable). vCloud Air provides a pool of vCPU, vRAM, Network and storage on the shared physical infrastructure. vCloud Air provides the required location independence and requires that the customer directly specify location of the datacenter that will host their cloud at time of instantiation. Note VMware's SaaS is also Not Applicable.	
FireEye	The FireEye cloud infrastructures consists of web and application servers, operating systems, and databases in a hosted environment and are comprised of both physical and virtual devices.	

	Computing power and resources are load-balanced across infrastructure and replicated to redundant datacenters in the event of a disaster. Client-specific data stored in databases are logically separated from other clients' data providing segmentation and isolation.
VirtueStream	Key to Virtustream solution is its proprietary and patented solution of uVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level. The resources are pooled based on two specific criteria: •ONLY Accessible Using Private Network – We call this pool "Enterprise" which most of Virtustream's IaaS workload is residing. There is no direct access from Internet into this pool. This is protected via a pair of routing and firewall from any other zones.

8.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

CA	APM	CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon's infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.
	MAA	The pool of web and application servers can be grown or shrunk when necessary. Any changes to the size of the pool remains transparent to end-users and customers, and would only be done by CA MAA systems administrators.
	CA Agile	This is a SaaS service, therefore, CA monitors all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. Data storage and network capacity are monitored and scaled to meet current client demands. Compute resources are scaled to meet client processing requirements
	ASM	All ASM core servers are dedicated physical servers; there is no elasticity. The ASM Public Status Pages are served from web servers in the Amazon Cloud, and the pool of web servers can be grown or shrunk if necessary. Any changes to the size of the pool would be transparent to end-users and customers, and would only be done by CA ASM systems administrators. Since this is a SaaS environment the CA SaaS Operations and delivery along with RackSpace are responsible for management of the capacity and monitoring.
Google	Saas, Google Apps can scale from 1 user to tens of thousand users. The usage of the services included are designed to horizontal scale within the confines of the per user storage allocation. Google Apps can be purchased with a 30gb per user allocation or with unlimited storage. Paas/IaaS, Google Cloud Platform was designed to scale on demand both in terms of available resources for applications designed and running on Google App Engine but also Compute Engine resources and more.	
AODocs	AODocs can scale from one user to tens of thousand users. The storage is based on the Google Apps storage which could be from 30Gb to unlimited storage depending on the Google Apps subscription.	
Virtru	Presently we over-provision services by 2.5x peak traffic in order to handle spikes. We are in the process of implementing horizontal scaling of all services and expect to have that work completed in the second half of 2016.	
Salesforce	User AuthenticationLogon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session.	

	Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application. In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce. Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce. Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.User ProvisioningUser provisioning and management is performed through the Salesforce Administrative Setup environment and is performed by Salesforce customers. Users, their profiles, permissions and passwords may be managed, edited, activated and deactivated as needed by those with appropriate permissions. An administrator (appointed by the customer and not by Salesforce) with appropriate privileges can manage session timeout, password policies, IP range login restrictions, delegated authentication/SSO, and requirements as part of this process. On first time login or password reset request, users are required to change their passwords to gain access. Salesforce also offers delegated authentication, enabling customers to provision and deactivate users from an external directory service.User Access ProfilesSalesforce enables administrators to manage roles and relationships between roles from within the application, in a single easy to read page depicting the role hierarchy. All users and application-level security are defined and maintained by the organization administrator and not by Salesforce. The organization administrator is appointed by CSBS. An organization's sharing model sets the default access that users have to each other's data. There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security. Details about sharing models and sharing model elements are provided below: Private Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.

	Public Read Only All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records. Public Read/Write All users can view, edit, and report on all records. Public Read/Write/Transfer All users can view, edit, transfer, and report on all records. Only available for cases or leads. Profiles A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control: Standard and custom apps the user can view (depending on user license) Service providers the user can access Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) Administrative and general permissions the user has for managing the organization and apps within it Object permissions the user is granted to create, read, edit, and delete records Page layouts a user sees Field-level security access that the user has to view and edit specific fields Record types are available to the user Desktop clients users can access and related options Hours during which and IP addresses from which the user can log in Apex classes a user can execute Visualforce pages a user can access User Roles Every user must be assigned to a role, or their data will not display in opportunity reports, forecast rollups, and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the company, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary. Record Types If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions. Field Level Security Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.

	The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.	
ServiceNow	ServiceNow is a multi-instance architecture that gives every customer its own unique database, which means that it is impossible for your data to be commingled with any other customer. The multi-instance architecture is not built on large centralized database software and infrastructure. Instead, we deploy instances on a per-customer basis, allowing the multi-instance cloud to scale horizontally and infinitely. For our multi-instance cloud, we deploy separate application logic (Apache Tomcat Java Virtual Machines) and database processes (MySQL) for every customer. This allows ServiceNow to scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.	
QTS	Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly out ward and in ward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. Delivering scalable, secure, high-performing, virtual data centers for government applications QTS is committed to not only giving your cloud the most secure home, but also the ability to utilize best-of-breed technologies. Flexible, high-performing, future proof infrastructure: Built upon the VMware vCloud® Suite, you'll benefit from reliable, high-performing infrastructure using a platform that includes VMware, EMC and Cisco. This compatible solution easily integrates with private VMware environments and provides a pathway to a hybrid cloud.Our scalability increases agility, efficiency and productivity: Your technologists can focus more time on your business and customers, and less time on your infrastructure. Rapid provisioning and improvements in utilization enhances your speed to market, delivers applications faster, and gets projects out the door. Virtually unlimited bandwidth and communications diversity QTS operates carrier-neutral data center facilities. This means that customers can select their communications service providers from hundreds of carriers, Internet Service Providers, dark fiber and satellite companies to meet their transport requirements. Selecting a provider from such a broad list of options gives customers exceptional route diversity and pricing options, as well as different Service Level Agreements and installation schedules. Customers who need very high amounts of bandwidth to conduct their business efficiently will never have to worry about running out of capacity at a QTS facility. Similarly, customers who require exceedingly high communications security have the benefits of selecting from physically diverse routes between their ends points and dark fiber that is not shared with any other users. In short, there are virtually no limitations to the type, amount, or security of communications available at each QTS data center facility.	
SAP	Ariba	There are no scalability limits with our products. We can scale accordingly to fit any data amount or user volume scenario.
	Fieldglass	The hosted Fieldglass solution can be horizontally and vertically scaled very quickly as the web server farm is fully virtualized. Only the SQL server is bare metal by design.
	Hanna	SAP HEC can be rapidly scaled to provision infrastructure & services on demand per customer requests.
	SuccessFactors	Our solution was designed and developed, from the outset, to be a highly scalable application. We also use the concept of "PODS," from a hardware perspective. A POD is a fault tolerant cluster of application & DB servers

		designed, as a scalable unit, to provide core processing and data storage services for fixed increment of customers. Attributes include: A POD is designed to support millions of subscribers. Our current 2nd Generation POD is scaled to 5M+ Multi-Vendor High Performance Blade Servers with 40GBps backplane fabric interconnects Multiple redundant Application Engines Clustering for availability and performance Hardware load balancers to route each new incoming session to the most available web and application processor Designed to support a high rate of concurrent connections while maintaining sufficient redundant capacity to meet SLA requirements New production PODs undergo a verification process before being brought into service Excess capacity PODs are always available on standby (scalability-on-demand) We will increase capacity if data center utilization surpasses the 70% threshold
VMware	All vCloud Air offerings partially comply with Rapid Elasticity. vCloud Air can be purchased as a pool of vCPU, vRAM, Network and Storage on shared or dedicated physical infrastructures that can be elastically provisioned and released. VMware's vCloud Air On Demand is fully compliant because capabilities can be elastically provisioned and released. VMware's SaaS Products i.e. AirWatch, does comply but the NIST requirement is not relevant to SaaS offerings. Note the vCloud Air Hybrid Cloud Manager is not Applicable.	
FireEye	FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure secure operation and available of the system. Capacity is actively monitored and pro-active upscaling is conducted to ensure resources are always available to end-users. Procedures are in-place for rapidly adding resources in the event the infrastructure approaches capacity.	
VirtueStream	Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for State of Utah allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool. Resources can be scaled based on application size, memory, storage, network requirements. xStream utilizes a supply chain to define resource profiles, attributes and offerings than can be provisioned.	

8.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

CA	APM	Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity. This portion is handled for the underlying cloud infrastructure by AWS with active participation by CA including escalations of issues.
	MAA	CA MAA systems administrators track the resource consumption of each virtual machine in use. ITIL flows are utilized to ensure service delivery. MAA customers do not need this information in order to use the service, nor do they have access to view it.

	CA Agile	Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity CA's best-of-breed monitoring solutions are deployed and supplemented with vendor specific diagnostic tools where appropriate 24x7 staffed network operation center (NOC) to analyze and respond to automated monitoring alerts
	ASM	CA ASM systems administrators track the resource consumption of each virtual machine in the cloud. Since this is a SaaS service, ASM customers do not need this information in order to use the service, nor do they have access to view it.
Google	Saas, Google Apps is already optimized for unlimited use by all end users. Google ensures high availability, low latency and fault tolerance as a part of the contracted services. No metering or rate limiting would be required as Google does not charge based on bandwidth use. Paas/IaaS, Google Cloud Platform includes application development tools, Google App Engine, compute resources, Compute Engine and Container Engine, data storage solutions and networking solutions. The pricing model is based on actual usage and that usage can be monitored with Google's Cloud Monitoring Service which also includes options to autoscale a project.	
AODocs	AODocs is already optimized for unlimited use by all end users. AODocs ensures high availability, low latency and fault tolerance as a part of the contracted services. No metering or rate limiting would be required as AODocs does not charge based on bandwidth use.	
Virtru	All services in our system monitored for availability, stabiity, security, and intrusion using a combination of tools, such as Dtrace, LogTrail, CloudWatch, DataDog, ElasticSearch and AlienVault.	
Salesforce	Subscription-based Service The Salesforce PaaS and SaaS offerings are subscription based and in a per user/month or user/year format billed annually with some of our products offered as total logins per month or by defined number of members billed annually. Bandwidth Salesforce is designed to use as little bandwidth as possible so that the site performs adequately over high-speed, dial-up, and wireless Internet connections. While average page size is on the order of 90KB, Salesforce uses compression as defined in the HTTP 1.1 standard to compress the HTML content before it is transmitted as data across the Internet to a user's computer. The compression often reduces the amount of transmitted data to as little as 10KB per page viewed due to the lack of image content. The site was designed with minimum bandwidth requirements in mind, hence are extensive use of color coding instead of images. Our average user also is known to view roughly 120 pages from our site per day. Our application is stateless; therefore, there are no communication requirements in the background once the page loads, like traditional client server applications, e.g., Outlook. Therefore, once the page loads, there are no additional bandwidth requirements until a user queries or writes information to Salesforce. System Overview In addition to our Trust site (http://trust.salesforce.com/trust/status), you will also have access to a System Overview, which will help Salesforce customers monitor performance and usage of their own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used Licenses API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages	

	Portal The above list is of all the possible metrics that Salesforce customers may have in their system overview.	
ServiceNow	ServiceNow is a subscription service measured by number of user accounts or number of managed nodes. ServiceNow has a documented capacity-planning model, which is used to determine sizing requirements and scaling options. The need to address capacity and horizontal system scaling is in the background, transparent to our customers.	
Docusign		
QTS	Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability 1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.	
SAP	Ariba	We have an Internal Tools Development Team which has established active monitoring systems with alerting and automated escalation. This includes log monitoring from the backend of the systems and this is tied to established internal processes related to security incident management. The environment, policies, tickets and reports are reviewed under ISAE 3402 assurance audit every six months.
	Fieldglass	Fieldglass utilizes various methods to ensure the system is available and is operating as expected. • Our network performance monitor ensures that all servers and devices are available and performing as expected. • All devices and servers on our network log into our enterprise SIEM tool. All activity is monitored by the Fieldglass security team to ensure activity does not vary from our known baseline. • An Active Performance Monitor has been built into the Fieldglass system. This monitor logs all system activity and enables Fieldglass engineers to drill into data such as concurrent user count, thread count, memory, CPU, SQL duration, server duration, client duration, page hits, etc. This data can be drilled into by day, hour, minute, server, and user. • Customer SLAs are tracked and communicated on a monthly basis. For 2015 we have a 99.4% success rate in meeting all customer page response time SLAs.
	Hanna	SAP HEC services are measured via SAP solution manager and reports are shared with the customer on a monthly basis as well as via self-service reports. SAP HEC operations team monitors the customer landscape and any disruption is addressed after reaching out to the customer and associated approval.
	SuccessFactors	Our hosting sites are designed to accommodate customers desiring a high level of managed service performance. In order to achieve such a level of performance, proactive monitoring is available through a variety of on-line tools that are implemented and managed by Cloud Operations. At a customer management level, the Cloud Operations monitors a series of “key metrics” that measure the results of various processes involved in supporting the business operations and service reliability. These metrics include reports of transaction volumes, latency, system availability, capacity, change management, and help incident response times as compared with established service level goals and standards. To facilitate required system performance, we monitor and tune the use of resources, and makes projections of future capacity requirements. We employ

		a variety of services to monitor and enhance application performance. The network makes extensive use of high availability architecture, and is monitored on a 24x7 basis at multiple levels. We utilize real time web applications performance monitoring software to do the following: Sample web traffic in real time via performance analysis software Track web application errors, (e.g. http 4xx-5xx errors) Monitor end-to-end user performance trends Detailed session analysis for session troubleshooting This data is reviewed on a daily and weekly basis by Operations Support, and is further supported with automated alerts. We proactively gather performance statistics, set triggers to alert on capacity thresholds, and regularly review utilization trends for capacity planning.
VMware	VMware's provides automatic monitoring and metering services to their IaaS and SaaS offerings. Note the vCloud Hybrid Manager is not applicable as it is not metered, because it is for management.	
FireEye	FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure secure operation and availability of the system. An internal monitoring system operates 24 hours per day to assess system availability and performance. The system is configured to send email alert notifications to FireEye operations personnel on a real-time basis communicating potential issues with the production systems.	
VirtueStream	The fundamental of Virtustream solution is based on uVM Technology, which is very unique in terms of billing. Virtustream solution takes average consumption of compute resources, and State of Utah would only pay for actual resources based on a monthly average. This is in comparison with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the Virtustream solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, Virtustream can provide consultative and project support based on time and materials. The µVM brings significant benefits: enabling application level performance SLAs – which an average VM cannot. µVMs eliminate wasted headroom in fixed size VMs, generating significant efficiency improvements (up to 40% beyond traditional virtualization) and Virtustream only charges by the µVM so you only pay for the resources you actually consume not what you might need. Using µVMs also enables applications to be used across multiple hypervisors, across multiple clouds and between different locations – enabling true hybrid clouds. µVM technology allows Virtustream to offer enterprise class clouds capable of running both mission-critical enterprise applications and web-scale applications, delivering the full benefits of cloud to the enterprise.	

8.1.3 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

CA	APM	In addition to the APIM SaaS offering CA Technologies also offers educational services and consultancy services. CA provides education and training services to its clients.
	MAA	CA MAA helps app developers visualize, investigate, manage, and support user interactions with their mobile apps. It provides deep insights into the performance, user experience, crash, and log analytics of mobile apps. CA MAA is aimed to help

		enterprises understand the experience of mobile app users across the DevOps application lifecycle. Enterprises can accelerate the delivery of user-experience-focused mobile applications and can achieve faster time to market by continuous application delivery while ensuring robust security.
	CA Agile	We provide a SaaS offering that is generally used to document and manage work within the SDLC. In addition to the CA Agile offering CA Technologies also offers educational services and consultancy services
	ASM	CA ASM is a SaaS offering that provides customers with the ability to monitor the availability, health, and performance of network services (web sites, email servers, etc.).
Google	Education SaaS offering - Google Apps for Education Messaging SaaS offering - Google Apps for Work, Google Apps Unlimited Collaboration SaaS offering - Google Apps Unlimited Identity Management SaaS offering - Google Apps SSO eDiscovery/Archving SaaS offering - Google Apps Vault Application Development PaaS - Storage IaaS offering -	
AODocs	AODocs Team Folders AODocs Document Management AODocs Retention Application AODocs Email Connector	
Virtru	SaaS email encryption and SaaS file encryption.	
Salesforce	Salesforce is the enterprise cloud computing leader dedicated to helping companies and government agencies transform into connected organizations through social and mobile technologies. Over 150,000 Salesforce customers across nearly every industry have successfully transformed their operations including over 1000 government agencies, representing all federal cabinet level agencies and the majority of the United States. Customer examples include: State of Texas, State of Colorado, State of California, GSA, USDA, USAID, and others. Salesforce was named one of the World's Most Innovative Companies by Forbes for the last five years in a row. Salesforce is #1 in Enterprise Cloud Computing and #1 in CRM according to IDC. Salesforce ranks as the Leader in the Gartner Magic Quadrant for "CRM Customer Engagement Centers" (SaaS), "Sales Force Automation" (SaaS), and "Enterprise Platform as a Service" (PaaS). Government agencies are using Salesforce PaaS and SaaS solutions for a multitude of government functions including grants management, constituent communications and correspondence management, incident and case management, call/contact center management, outreach programs, learning management, volunteer management, project management, and even donor management, among numerous others.	
ServiceNow	SaaS Offerings: •Cloud and Infrastructure Management Tools •Customer Relationship Management •Project and Portfolio Management (PPM) Tools •Security •Workflow and Electronic Signature •Proposed new category: Information Technology Service Management Tools	

QTS	QTS has built some of the world's largest, most robust, and redundant data centers. The company's innovative 3C product set of custom data center, colocation, and cloud and managed services provides a fully integrated platform and a flexible, scalable level of service that is difficult to match. Our service categories include: IaaS Custom Data Center IaaS Enterprise Cloud IaaS Managed Cloud IaaS vCGS Cloud IaaS Federal Solutions IaaS Healthcare Solutions IaaS Financial Service Solutions Colocation Connectivity Critical Facilities Management Hybrid IT Solutions Disaster Recovery as a Service (DRaaS) Managed Services: Managed Hosting, Managed Network, Managed Systems, Managed Security, Managed Storage & Backup, Managed Disaster Recovery, Data Security	
SAP	Ariba	We provide solutions that allow enterprises to efficiently manage the purchasing of non-payroll goods and services required to run their business. We refer to these non-payroll expenses as "spend."" Our solutions include software, network access, and expertise. They are designed to provide enterprises with technology and business process improvements to better manage spend and, in turn, save money. Our solutions streamline the business processes related to the identification of suppliers of goods and services, the negotiation of the terms of purchases, and ultimately the management of ongoing purchasing and settlement activities. Our solutions allow enterprises to take a systematic approach with products and services that work together. By combining software, network access and professional services into a comprehensive solution, we help customers to address six key areas of spend management: Visibility - enhance spend visibility and control across spend categories, disparate systems and corporate divisions Sourcing - identify top suppliers, negotiate procurement terms, leverage aggregate spend, and manage procurement contracts Contract Management - streamline and automate from contract creation to compliance Procurement – streamline requisitioning and procurement across all types of spend Invoice and Payment - automate invoicing and payment processes Supplier Management - optimize buyer-supplier interactions throughout the spend lifecycle
	Fieldglass	The SAP Fieldglass Vendor Management System (VMS) application is a workforce management SaaS offering.
	Hanna	HANA Enterprise Cloud is a private managed cloud primarily for all SAP enterprise-wide SAP applications such as: ERP, CRM, SRM, BW, etc. All SAP applications can be hosted in HANA Enterprise Cloud (via BYOL or Subscription Licensing model)
	SuccessFactors	Our original product release dates are as follows:

		Performance Management – 2001 Goal Management – 2002 360/Multi-Rater Reviews - 2002 Succession Management - 2004 Compensation Management – 2004 Analytics & Reporting – 2005 Learning & Development – 2006 Recruiting Management – 2006 Variable Pay Compensation – 2007 Employee Profile – 2007 Stack Ranker – 2008 Employee Central – 2009 Metrics Navigator – 2009 Goal Execution – 2010 Calibration – 2010 Workforce Planning (Acquisition) – 2010 Workforce Analytics (Acquisition) - 2010 Plateau LMS (Acquisition) – 2011 JAM – 2011 Employee Central Payroll – March 2012 Onboarding (acquisition of KMS) – May 2013
FireEye	FireEye is offering 4 distinct cloud solutions that can be classified into the following service categories and sub-categories: 1.Email Threat Prevention (ETP) Security – SaaS 2.Mobile Threat Prevention (ETP) Security – SaaS 3.Threat Analytics Platform (TAP) Threat Intelligence – SaaS 4.FireEye as a Service with Continuous Vigilance (FaaS CV) Managed Security Service – SaaS	
VirtueStream	Virtustream is an Infrastructure as a Service (IaaS) offering focused on mission critical workloads and applications. The solution provides as part of the response is IaaS only. Virtustream's IaaS is targeted for all virtualized, x86 based cloud solution. While we have secured and segmented infrastructure for FedRAMP, FISMA, PCI and other regulated workload, it is best suited for any and all enterprise workload as long as the workload can be virtualized and run on x86 platform. For non x 86 environments, Virtustream provides Collocated areas, which is cross connected with the cloud.	

8.1.4 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

Carahsoft complies with the requirements in attachment C & D. Cloud service models by vendor are broken out in section 6.6 of this response per the request in attachment C.

8.1.5 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Carahsoft's cloud vendors fit into multiple categories as listed out in Attachment D. Many of our vendors fit a hybrid cloud deployment method with ability to silo off a private cloud if security needs dictate such. Our cloud vendors are broken out by service model in section 6.6 of this response. Carahsoft's cloud vendors

also fit into many categories as listed in section 1.1.3 of Attachment D. Depending on the type of data and service requested our vendors can support everything from on demand self service delivery to a completely managed and measured service option.

8.2 Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Carahsoft will be utilizing Subcontractors to provide services and solutions for specific manufacturers within this response. In other cases, Carahsoft will work with the manufacturers to provide these services and solutions to all Participating Entities. All Subcontractors shall be vetted to ensure they have the necessary qualifications to do business within the State of Utah and any applicable Participating States. All Subcontractors will also comply with the applicable terms and conditions of the RFP and subsequent contract, as well as all Participating Addendums for the States they are subcontracting in.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Carahsoft will use subcontractors as a third party company to provide services in relation to the solutions provided by the manufacturer. No other functions of contract management or execution will be performed by the subcontractor. While Carahsoft cannot determine all roles and responsibilities of the positions for each subcontractor, there are multiple different standards which subcontractors utilize for these types of contracts. Here is an example set of the traditional roles a subcontractor would play on behalf of Carahsoft for this RFP:

Job Title: Consulting Engineer
Functional Responsibility: Working under close supervision, person provides technical or scientific and project support for multiple large-scale projects that cross-cut multiple specialization and product development areas. Applies advanced business and/or technical expertise to assist others with defining, analyzing, validating and documenting complex customer operating environments, states of technology and current engineering processes. Provides advanced technical support to others involved in applying specialized knowledge to complex customer processes and requirements. Supports complex technical investigations through advanced research techniques, analysis or development phases of engineering projects. Works with other engineering disciplines in the development and application of processes to improve quality, reliability, cost customer appeal, and satisfaction.

Job Title: Project Manager

Functional Responsibility: Possesses a thorough understanding of the process requirements and provide both technical and management oversight of the project. Responsible for customer satisfaction, serves as the single point of contact, compliance with the Statement of Work, project planning and management, resource allocation, and reporting.

Job Title: Senior Information Architect
Functional Responsibility: Provides supervision, person designs Intranet/Internet/Extranet architectures and develops implementations plans; administration activity; i.e., hardware, security, firewalls. Implements security architecture using LDAP, SSL and firewalls. Installs, configures and maintains all Intranet/Internet/Extranet tools, databases and features; provides support to e-commerce and other systems. Implements server design, development, and operation as well as analyze and develop requirements for hardware sizing/capacity, data validation, security and integration points to other applications.

Job Title: Information Architect
Functional Responsibility: Designs Intranet/Internet/Extranet architectures and develops implementations plans; administration activity; i.e., hardware, security, firewalls. Implements security architecture using LDAP, SSL and firewalls. Installs, configures and maintains all Intranet/Internet/Extranet tools, databases and features; provides support to e-commerce and other systems. Implements server design, development, and operation as well as analyze and develop requirements for hardware sizing/capacity, data validation, security and integration points to other applications.

Job Title: Senior Consulting Engineer
Functional Responsibility: Provides supervision, person provides technical or scientific and project support for multiple large-scale projects that cross-cut multiple specialization and product development areas. Applies advanced business and/or technical expertise to assist others with defining, analyzing, validating and documenting complex customer operating environments, states of technology and current engineering processes. Provides advanced technical support to others involved in applying specialized knowledge to complex customer processes and requirements. Supports complex technical investigations through advanced research techniques, analysis or development phases of engineering projects. Works with other engineering disciplines in the development and application of processes to improve quality, reliability, cost customer appeal, and satisfaction.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Carahsoft will be making the determination of what subcontractors to include on the NASPO ValuePoint Cloud contract upon time of award. Carahsoft will ensure a subcontractor has all of the necessary certifications to do business in the State before adding them to the contract as a subcontractor. In addition, Carahsoft will do credit checks and meet with the subcontractor on multiple occasions to confirm that they are reliable and exceed expectations as a services and solutions provider. Finally, an agreement will be put in place between Carahsoft and the subcontractor to ensure optimal efficiency with the subcontractor's responsibilities.

A subcontractor will be actively involved in understanding and shaping any Statements of Work created for the services of a deal in order to make sure that they have the capacity to meet all of the necessary requirements. These Statements of Work will dictate the terms upon which the subcontractor is deployed for services, so Carahsoft will work specifically with subcontractors that are active in the public sector and understand the nuances of selling to government entities.

8.3 Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

Security is of the uptmost importance to all of the Service providers that Carahsoft is submitting. Should and actual breach occur, it is the first priority of Carahsoft and the service provider to identify the source of the breach and implement safe guards to prevent one from happening in the future. The Service Provider will promptly notify the Purchasing Entity of the incident. Notification of the breach will be provided by the service directly to the security or customer contact that is identified by the Purchasing Entity. Methods of communication could include phone or email notification.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Carahsoft ensures that no unwanted marketing efforts are made to customers through an easy to manage opt out system in our database. Carahsoft can also limit communications by vendor to ensure that only those vendors approved by the customer reach out with marketing materials or product updates. Carahsoft will never support or assist in the pushing of adware or unwanted software to participating customers.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

For applicable cloud offerings, user test/ staging environments are available that are identical to real-time production environments.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are be accessible to people with disabilities, and must comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable.

The user interfaces provided for within this proposal are accessible to people with disabilities using assistive technologies.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

All cloud solution offerings within this proposal that are delivered via web browsers are accessible using current releases of common internet browsers such as Internet Explorer, Firefox, Chrome, Safari, and more.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Upon request of the customer, Carahsoft can host meetings via Adobe Connect web conferencing software or travel in person if the need presents itself. Carahsoft is happy to support and comply with any regulations or sensitive data compliance needs that the customer identifies. Carahsoft has the ability to limit customer information to a secure and isolated database if needed.

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Project scheduling and work planning documents are developed in conjunction with customer requirements. Project planning activities are conducted with a focus on developing a statement of work that defines deliverables, customer and contractor areas of responsibility, as well as project benchmarks, and deadlines. Project complexity and customer requirements determine the overall timelines for development, testing, and solution implementation.

8.4 Customer Service

8.4.1 Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

The core of Carahsoft's business is to provide the best customer service to our government customers and vendor partners. We are an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading software license GSA resellers. Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 56,000 orders in 2014 that were each completed the same day received. Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Associated with all contracts are dedicated and experienced contract management resources. Quality and accuracy is the driving factor behind Carahsoft's successin the government market. All solutions proposals and price quotes that are sent to our customers go through a three step review process for quality. The first is a pricing review that is automatically run against the pricing database to ensure pricing accuracy for the proper contract. The second review is at the certified Account Representative level who will check pricing and configurations for accuary and also review any SOWs that are included. Finally, mangagement review confirms the quality and accuracy of the proposal that will be sent to the Purchasing Entity. Carahsoft has instituted an escalation procedure for any problems or complaints that may arise. There are four levels of escalation and include review by the Account Representative assigned to the

Purchasing Entity, followed by the Regional Manager of the territory, next to the Vice President of State and Local and finally to the President/CEO. Each stage of escalation shall have a response SLA of no more than 24 hours.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.
c. Customer Service Representative will respond to inquiries within one business day.
d. You must provide design services for the applicable categories.
e. You must provide Installation Services for the applicable categories.

Carahsoft confirms and agrees that we will name a lead representative for each Participating Addendum. The contact information will be listed on the Carahsoft website and kept current. Carahsoft confirms it will have a representative available by phone and email available 7am-6pm on Monday through Sunday in the applicable time zones. Carahsoft confirms that it will respond to all inquiries within one business day or sooner. Carahsoft will engage with our service providers to provide design services in the applicable categories Carahsoft will engage with our service providers to provide installation services in the applicable categories.

8.5 Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Security is of the utmost importance to Carahsoft and our service providers. As an example of our Service Provider's security standards, please see the government security response for Salesforce: Government Trusted Security and Infrastructure
Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com gives you the peace of mind only a world-class security infrastructure can provide.

Third-party validation
Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Protection at the application level

Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.

Protection at the facilities level
Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center.

Protection at the network level
Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance
- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Carahsoft is happy to support and comply with any regulations or sensitive data compliance needs that the customer identifies. Carahsoft has the ability to limit customer information to a secure and isolated database if needed. Under no circumstances will Carahsoft ever publish or release secure customer data. Carahsoft's cloud vendors are all FIPS certified or have equivalent security standards in place to ensure no customer data is released outside of the secure cloud.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Carahsoft will use customer accounts and data only in the processing of an order and management of the customer's service entitlements. Carahsoft's vendors, as outlined in their specific Master Agreements, only us customer account data for the express purpose of providing the service to the customer. Included in that service is implementation, technical support, and training efforts. Under no circumstances will Carahsoft or its cloud partners use customer information outside of normal operating procedures.

8.6 Privacy and Security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

CA	APM	CA technologies understands that security is a top concern when evaluating cloud-based applications, which is why CA technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis.
	MAA	
	CA Agile	We use CIS and NIST standards as baselines for hardening our systems. We are currently working towards a NIST 800-53r4 certification however this is not yet complete. We are continuously reviewing our compliance with these standards. We perform monthly scans against our Production Infrastructure based on CIS standards. We scan for both vulnerabilites and compliance best practices bases on NIST 800-53v4 standards. Vulnerabilites are tracked and remidiated based on severity and risk.
	ASM	Please see our response to APM/MAA
Google	Google's currently maintains a FedRAMP Authorization to Operate. FedRAMP incorporates the relevant NIST SP and FIPS security requirements. Further, Google contractually commits to maintaining SOC2 and ISO27001 certifications.	
AODocs	AODocs is committed to comply SOC2 type 2.	
Virtru	Virtru's business depends on its ability to support healthcare and criminal justice markets, which requires us to maintain compliance with HIPAA and CJIS standards which both make extensive use of NIST standards	
Salesforce	On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4. Salesforce provides contractual assurance to its customers that the Customer Data hosted in Salesforce's services will be kept confidential and not accessed by third parties except under narrow circumstances (such as a customer support issue or as required by law). In the case of customer support, the company's personnel will access a customer's Org only with prior approval and subject to confidentiality obligations.	
ServiceNow	ServiceNow is a cloud service provider offering a SaaS solution deployed from a private cloud that meets the five essential characteristics of cloud computing as described in 8.1. ServiceNow applies the same data classification for all hosted customer data. ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify	

	customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data controller for all data placed into their instance. ServiceNow does not examine, inspect, monitor or analyze customers' data. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.	
QTS	QTS understands the growing number of requirements along with the complexity of managing the high cost-risk if you are not in compliance, and makes compliance a top priority. Our dedicated QTS Internal Audit team is focused on helping you define controls and processes to meet your ever-expanding compliance requirements. We are steadfast in protecting your data with the commitment to allocate required resources, technology and controls to not only help you achieve and maintain compliance today, but to expertly support your needs as they inevitably grow and change in the future. QTS tackles compliance differently. We provide a flexible, integrated approach to meet the IT compliance and regulatory needs across a wide variety of industries – from Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) to U.S.–EU Safe Harbor. Our approach reduces the complexity and workload to effectively support their compliance efforts.	
SAP	Ariba	Our security framework, which consists of semi-annual independent third party AICPA audit under the Trusted Services Principles of security, confidentiality, process integrity and availability as well as annual certification by an independent Qualified Security Assessor for PCI DSS, is highly aligned with the NIST controls. Our security framework and cloud services are designed to receive process and store data sets of a commercial business-to-business nature and are multi-tenant and international in scope. FISMA/NIST is designed to protect US government data that can include classified information as well as sensitive PII such as ePHI and SSN's or government identifiers. We practice data avoidance where these data sets are concerned primarily to reduce the risk to us and to our customers but also to avoid additional regulatory compliance which has onerous reporting and high costs which would have to be passed on to our customers. Where FISMA regulated entities can take advantage of our solutions, the data sets they expect to store must be validated to avoid being under regulatory requirements beyond what we can provide in terms of both security as well as reporting.
	Fieldglass	Fieldglass has based its security program on the ISO 27002 security standard and has maintained its ISO 27001 certification since February 2011. However, to ensure that a robust security framework was developed, additional controls were added and/or modified based on COBIT DS5 Ensure Systems Security, specific NIST special publications, and vendor specified best practices. Fieldglass uses a SSAE 16 audit with a twelve-month audit cycle to validate that the controls defined within the security framework are operating effectively.
	Hanna	SAP will show the compliance with the SAP Cloud Security Framework by the compliance audits and/or certification audits only as it pertains to the HANA Enterprise Cloud. SAP Cloud and Infrastructure Delivery's Security, Risk & Compliance Office has developed the Integrated

		Information Security Management System (IISMS) Framework. The IISMS Framework is based on SAP's corporate quality and security policy as well as the corporate security standards and guidelines relating to information security and business continuity. This IISMS Framework was adapted to SAP Cloud Security Services as SAP Cloud Security Framework (Cloud SFW). SAP's security, process and compliance team conducts technical security audits to validate that security concepts have been implemented successfully and to safeguard the usage of newly developed tools. Compliance Audits Cloud solutions from SAP have passed ISAE3402/SSAE16-SOC 1 Type II and/or SOC 2 Type II audits (in the following referred to as SOC audits) and can provide the related audit reports on request. Certification Audits The SAP HANA Enterprise Cloud has attained certifications according to the following ISO standards are available (related audits are in the following referred to as ISO audits): • ISO 27001:2013 • ISO 22301:2012 • ISO 9001:2008
	SuccessFactors	Our IT architecture is aligned with ISO 27002. We are Safe Harbor certified and in alignment with BS10012 and ISO 20000 for Service Delivery. We demonstrate an on-going commitment to protecting the confidentiality, integrity and availability ("CIA") of data from internal and external threats, making us a reliable and secure system provider. Our secure multi-tenant Software as a Service (SaaS) platform is designed for availability, security, scalability, and performance. Industry best practices and standards are adopted and incorporated. Our Network also complies with the Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We provide privacy compliant data center facilities not only in the United States but also as a Member State of the European Union (EU) or a state of the European Economic Area (EEA). Currently, such data centers are certified for ISO27001, ISO9001 and PCI-DSS compliance. Our security services provide complete and thorough monitoring of all traffic on the network on a 24x7x365 basis, and include security technology, alert services and incident management support. We are audited twice annually to SSAE16 (US) or ISAE 3402 (international) accounting standards.
VMware	VMware is fully committed to complying with NIST and all other relevant industry standards including FedRAMP, FISMA, PCI, CSA CAIQ, etc. This is demonstrated by VMware's track record of pursuing and obtaining certifications such as those listed above. vCloud Government Service has been certified to store and secure Low Risk Level and Moderate Risk Level data as defined by FIPS PUB 199. In addition, VMware is capable of enhancing the vCloud Government Service to meet participating State's requirements to be able to store data that is defined by FIPS Pub 199 as High Risk Data. VMware is committed to maintaining compliance with all of our existing and future compliance certifications. Our ability to remain competitive as a software and services provider in the public sector depends upon it. Thus we have established a comprehensive security and compliance team to ensure that we maintain compliance as well as a strong security posture.	

	VMWare supports regular internal and external audits to ensure compliance with its certifications as required. The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53. Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits and have ISO 27001 certifications.
FireEye	FireEye has mature and well documented security and privacy programs. The programs include third party certifications for SSAE 16 SOC 2, FedRAMP certifications, Model clauses, Privacy and security standards among others. The data that FireEye receives is only in conjunction with the malware analysis.
VirtueStream	The Virtustream Federal Cloud (IaaS) has met the requirements for a FedRAMP moderate P-ATO. The IAAS is assessed annually by a FedRAMP certified 3rd Party Assessment Organization (3PAO). The annual assessment will review a subset of the NIST 800-53 Revision 4 controls as designated by FedRAMP. Virtustream's 3PAO shall demonstrate impartiality throughout the assessment to accurately assess the status of all security controls in place.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits. The application currently does not hold a Soc 2 attestation.
	MAA	CA MAA is certified for SOC 2 Type 1 Security Audit.
	CA Agile	Our data center provider has a SOC 2 audit report that can be provided upon request. Our application does not currently have such certifications.
	ASM	Rackspace datacenters annually undergo various certification including SOC 3 audits. The application currently does not hold a Soc 2 attestation.
Google	Google has a FedRAMP ATO at the Moderate impact baseline. FedRAMP incorporates many NIST SPs and FIPS including 800-53, FIPS 199, FIPS 200), and has a specific offering. Google Apps for Education that is FERPA and COPPA compliant. Other compliance standards such as HIPAA and CJIS don't offer certification per se, but are commonly accommodated (i.e. Google will sign a BAA to meet HiTECH/HIPAA requirements, and has numerous customers who bear responsibility for meeting CJI processing requirements). PCI DSS is generally not applicable to SaaS systems (though we can do email hygiene processing to protect against incidental usage), but Google IaaS/PaaS does meet PCI DSS v3 standards. Google also holds and is committed to maintaining SOC2 and ISO27001 certifications.	
AODocs	AODocs doens't hold an HIPAA certifications per se, but are commonly accommodated to meet HIPAA requirements signing a BAA.	
Virtru	HIPAA, FERPA, CJIS, NIST 800-53, NIST SP-800	
Salesforce	Salesforce and the Salesforce Force platform is ISO 27001 certified and PCI-DSS compliant. SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include:	

	FedRAMP Authority to Operate from Department of Health and Human Services CSA 'Consensus Assessments Initiative' JIPDC (Japan Privacy Seal) Tuv (Germany Privacy Mark) TRUSTe HIPAA In provisioning and operating the services, Salesforce complies with the provisions of HIPAA's Privacy Rule and Security and the HITECH Act that are applicable to business associates. Salesforce's customers are still responsible for complying with the same in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. From a legal standpoint, some of our customers have asked Salesforce to assist them in meeting their compliance obligations; for example, by entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI). FERPA Salesforce maintains appropriate administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of data our customers submit to the Salesforce Services as Customer Data. Salesforce's customers are responsible for ensuring the security of their Customer Data in their use of the service and implementing any necessary customer-controlled settings. To aid, Salesforce offers robust security functionality that provides our customers the flexibility to use the application in a configuration that furthers compliance with local data protection laws and regulations. While Salesforce complies with applicable law in provisioning and operating the Salesforce services, it is the sole responsibility of Salesforce's customers to ensure compliance with applicable laws in their respective uses of the Salesforce services.PCI-DSSSalesforce is PCI Level 1 compliant and has received a signed Attestation of Compliance (AoC) for the Payment Card Industry Data Security Standard (PCI-DSS). Salesforce customers who must adhere to PCI compliance may store personal account numbers ("PAN" or "credit card numbers") in Salesforce, with the following caveats: - PANs may only be stored in a custom field encrypted via Classic Encryption or supported field types via the Platform Encryption functionality. PANs must not be stored in clear text fields, attached files, or any other location. - Customer administrators must configure Salesforce features to support their organization's PCI controls.NIST SP 800-171NIST Special Publication 800-171 is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies) for purposes unrelated to information processing. In other words, the nonfederal organizations are not operating their information systems to process agency data, including CUI, on behalf of the agency but rather for other purposes (e.g., when designing or producing an aircraft, performing a study, or conducting background investigations for security clearances). Salesforce recommends that its customers use the classifications as detailed in FIPS 199. FIPS 140-2, FIPS 197, FIPS 199, and FIPS 200 On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4.

	As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2/3 cryptographic implementations for data being transferred between the customer's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below. Data Transmission between the customer's web browser and Salesforce: Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048-bit Public Key. Our service uses International/Global Step Up certificates. We support one-way TLS, in which customers create secure connections before sharing private data. Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Data Transmission for Backup Media: Media containing customer data is not transported outside of controlled salesforce.com areas and therefore relies on physical access controls to protect the data. Data at Rest: NIST 800-53 Rev. 3 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data. Primary Data Storage: User passwords are stored in the RDBMS encrypted via the SHA algorithm with a 256-bit hash. This is a one way hash. The passwords are encrypted by the application. For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with Advanced Encryption Standard (AES) encryption (as defined by FIPS 197), for a selection of custom fields included in the Salesforce Platform and CRM applications. Field-level encryption ensures the data associated with designated fields is encrypted in storage.
ServiceNow	ServiceNow's security policy is based on ISO27001:2013 and has been since 2012. ServiceNow also has annual SSAE 16 SOC 1 Type 2 and SOC2 Type 2 attestations with controls being based off NIST 800-53. The ServiceNow Service Automation Government Cloud Suite is a FedRAMP Compliant Cloud System with a JAB Provisional Authorization. This cloud offering has regulatory restrictions to the types of tenants that can use it. ServiceNow's FedRAMP compliant and standard commercial datacenter environments are virtually identical. The differences that do exist, such as only allowing access to specially adjudicated US citizens, exist for regulatory reasons not because the environment is superior in some way.
QTS	QTS assists with mapping between DOD IT RMF/DIACAP and NIST as well as International Standards Organization (ISO) standards and many others. QTS maintains control mappings that include: • NIST 800-53/FedRAMP (Low/Moderate/High)

	• DOD IT RMF/DIACAP (MAC I/II/III Sensitive & Public) • HIPAA-HITECH-Omnibus • PCI-DSS • ISO/NATO • CNSS/ICD/DCID/NISPOM	
SAP	Ariba	We are audited and certified by independent third-party auditor PricewaterhouseCoopers (PwC) for compliance with ISAE 3402 SOC1 Type II, SOC2 and SOC3 every six months. Upon completion of the audit, an attestation letter is issued, stating our compliance. In addition, our primary hosting facility (Equinix) infrastructure is audited for compliance with SSAE 16 SOC1 Type II. The Service Organization Controls report (SOC) is aimed at three different audiences. SOC1 (aimed at financial auditors) is the same type of report as the SAS70 but also includes an attestation letter signed by both our company and the auditor. SOC2 is aimed at IT and security practitioners. The SOC3 is the publicly viewable web seal to show that we have been audited. In addition, we have attained PCI (Payment Card Industry) - DSS (Data Security Standard) certification as a Level 1 Service Provider and compliance with the Visa USA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program. These programs were created specifically for merchants and service providers who process, store, or transmit cardholder data. The PCI DSS is a set of comprehensive requirements for enhancing payment account data security which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. It was developed to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. CISP and SDP reflect Visa's and MasterCard's respective longstanding commitment to information security.
	Fieldglass	SAP Fieldglass has achieved the following certifications: • ISO 27001 • SSAE 16 SOC 1 and SOC 2 HIPPA Fieldglass does not store Protected Health Information (PHI) on its system and is not required to comply with the Health Insurance Portability and Accountability Act. PCI The Fieldglass application does not process credit card information. We are not (and are not required to be) PCI compliant.
	Hanna	Please see response to 8.6.1
	Hybris	The Savvis datacenter located in Boston, MA is SSAE16 Type II SOC I Compliant. This replaces the older SAS70 Type II audit standard.
	SuccessFactors	We have been audited to the SOC 2 Trust Services Criteria. This signifies that our control objectives and control activities have been examined by an independent accounting and auditing firm, and that these controls fairly presented the controls in operation as of a specific date and were suitably designed to achieve the control objectives. Our SOC 2 audits are conducted semi-annually (May, November) by PricewaterhouseCoopers (PwC). We also hold US Federal FISMA Moderate

		Authority to Operate with both OPM and NTIS. We are compliant with EU Privacy Directive 95/46/EC and are Safe Harbor self-certified. https://safeharbor.export.gov/companyinfo.aspx?id=26196We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor.
VMware	VMware IaaS Services ISO/IEC 27001: ISO/IEC 27001 is a globally recognized standard for the establishment and certification of an information security management system (ISMS). vCloud Air continues to maintain a current ISO/IEC 27001 Certification and has recently issued updated certification for ISO/IEC 27001:2013. Achieving certification means that VMware has implemented a holistic security program that conforms with the ISO 27001 standard requirements, both in the security management system and control activities. The audit of the ISMS was completed by Brightline CPAs and Associates - an ANAB accredited certification body. HIPAA: The Health Insurance Portability and Accountability Act of 1996(HIPAA), which has incorporated requirements from the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, established national standards for the security and privacy of Protected Health Information (PHI) in the United States. To help customers comply with HIPAA, VMware offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. The BAA was designed in conjunction with a leading law firm with expertise in HIPAA and provides fair and reasonable terms for healthcare providers, insurers, and other organizations. VMware has completed an independent third party examination of vCloud Air against applicable controls of HIPAA. SOC 1 (SSAE16/ISAE 3402): Service Organization Control (SOC) 1 reports are conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPS). The SOC 1 framework reports on internal controls over financial reporting for any service organization such as VMware vCloud Air. SOC 1 aligns to the International Standard on Assurance Engagements (ISAE) 3402 international reporting standards. SOC 1 examinations are specifically intended to meet the needs of the managements of vCloud Air's customers and vCloud Air's customers' auditors, as they evaluate the effect of the controls at vCloud Air on the clients' financial statement assertions. VMware has completed an independent third-party examination of vCloud Air which spans a twelve (12) month review period. SOC 2: The Service Organization Control 2 (SOC 2) report is composed of a comprehensive set of criteria on security, availability, processing integrity, confidentiality, and privacy and is similarly set forth by the America Institute of Certified Public Accountants (AICPA). The SOC 2 reports are	

	intended for use by stakeholders (e.g. customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls. VMware has completed an independent third-party examination of vCloud Air that also spans a twelve (12) month review period. SOC 3: Trust Services Report for Service Organizations Control 3 (SOC 3) reports are designed to meet the needs of customers who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy. vCloud Air has completed an independent third-party SOC 3 examination of VMware vCloud Air. SOC 3 is composed of a comprehensive set of trust principles including security, availability, processing integrity, confidentiality and privacy. Cloud Security Alliance: VMware vCloud Air has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). CAIQ provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. FedRAMP Provisional Authority: VMware vCloud Government Service, provided by Carpathian, now has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a ""do once, use many times"" framework that can reduce government organizations' costs, time, and staff required to conduct redundant agency security assessments. U.S. government agencies can now leverage vCloud Government Service to meet the stringent security and privacy requirements of FedRAMP. FIPS 140-2: VMware vCloud Government Service is fully FIPS 140-2 compliant including hardware which provides its 2-Factor Authentication capabilities. FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data. FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data. CJIS: vCGS recently underwent a CJIS assessment by CoalFire, Inc. CJIS is not a certification, it is a policy that must be followed and accredited for each deployment which requires it. The goal of VMware's CoalFire assessment was to create a baseline configuration that can be reused across any CJIS opportunity to accelerate the implementation and accreditation timeframes. FERPA: Like CJIS, FERPA compliance is assessed and confirmed for each deployment that requires it. VMware's vCloud Government Service FedRamp certification and others provide evidence that the underlying infrastructure is capable of meeting rigorous information security and availability requirements. VMware will work with Participating Entities to meet FERPA requirements on a task order basis. PCI Data Security Standards (DSS): Neither vCloud Air nor vCGS are currently PCI certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis. IRS Publication 1075: Because both IRS 1075 and FedRAMP are based on NIST 800-53, the compliance boundary for IRS 1075 is the same as the FedRAMP authorization. This, vCGS complies with IRS Publication 1075 on the basis that it is FedRAMP certified. FISMA: vCGS is FISMA Low and Moderate compliant.

	NIST 800-53: NIST 800-53 provides the core controls that must be met to achieve FedRAMP compliance. VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB), thus we are compliant with NIST 800-53. NIST SP 800-171: VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). NIST 800-171 outlines a subset of the NIST 800-53 requirements, and as stated above, VMware vCloud Government Service is compliant with these guidelines. Since NIST 800-171 outlines a subset of the NIST 800-53 requirements, VMware vCloud Government Service is compliant with NIST SP 800-171. FIPS 200: Neither vCloud Air nor vCGS are currently FIPS 200 certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis. VMWare AirWatch The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53. Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits.
FireEye	Currently the standards that apply are SSAE 16 SOC 2 Type 2, with a FedRAMP ATO in place and full FedRAMP certification in process. We are also in the process of becoming FedRAMP ISO 2700x certified.
VirtueStream	Security is the foundation of our business. Virtustream's xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain SSAE16, ISAE3402, PCI-DSS 3.0, FISMA, IS0 27001-2005/2013, ISO 9001-2008, HIPAA, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

CA	APM	CA technologies understands that security is a top concern when evaluating cloud-based applications, which is why CA technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis.
	MAA	All MAA core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The MAA dashboard and API are protected with HTTPS/TLS encryption, and users are required to authenticate in order to access these.
	CA Agile	We use a co-located data center provider and within that environment we have a dedicated cage to which only our Operations Team has access. We also monitor all traffic across our systems using HIDS (OSSEC) and NIDS (Snort) to notify of any suspicious activity.
	ASM	All ASM core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The ASM dashboard and API are protected with HTTPS/TLS encryption, and users are required to use a username and password to login to their accounts.

Google	In this DPA the obligations of Google to hold all customer data as confidential and wholly owned by the customer is detailed. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.
AODocs	AODocs being built in Google AppEngine and Google Drive.
Virtru	Please see the Virtru Security Policies and Procedures and the Virtru Privacy Policies and Procedures provided in the Supplemental Information section of this response.
Salesforce	Government Trusted Security and Infrastructure Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security. Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com gives you the peace of mind only a world-class security infrastructure can provide. Third-party validation Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe. Protection at the application level

	Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts. Protection at the facilities level Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center. Protection at the network level Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs. Secure Data Centers Data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Colocation data center personnel do not have network or logon access to the Salesforce systems. Colocation personnel have physical access to the Salesforce secure server room in the event of an emergency, but do not have keys to the individual racks containing hardware. Data centers maintain a common baseline of physical and environmental controls across data centers. The exterior perimeter of each anonymous data center building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned 24/7 guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and to the Salesforce secure rooms at all times. Access to Salesforce's secure server rooms in the datacenter is authorized based on position or role. Additional access controls enforced by an electronic key box are implemented for the dedicated Salesforce Government Cloud racks to ensure that access is limited to Qualified U.S. Citizens. Salesforce has an established process to review data center access logs to the server room. Additionally, an at least annual assessment of the data center is performed to ensure the data centers are meeting Salesforce's security control requirements. In addition to securing the data center locations, it is critical that the data center facilities maintain robust critical infrastructure to support Salesforce through the following services:

	Temperature and Humidity Controls • Humidity and temperature control • Redundant (N+1) cooling system Power • Underground utility power feed • Redundant (N+1) CPS/UPS systems • Redundant power distribution units (PDUs) • Redundant (N+1) diesel generators with on-site diesel fuel storage Secure Network Logistics • Concrete vaults for fiber entry • Redundant internal networks • Network neutral; connects to all major carriers and located near major Internet hubs • High bandwidth capacity Fire Detection and Suppression • VESDA (very early smoke detection apparatus) • Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression
ServiceNow	The ServiceNow cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability and security. ServiceNow's comprehensive approach to address this demand is enabled by the following: (a) ServiceNow's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery; (b) ServiceNow achieves flexibility and control in its ability to deliver a stable user experience to the customer by having a logical single tenant architecture; (c) ServiceNow's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering those applications in a reliable and secure cloud environment; (d) ServiceNow invests in a comprehensive compliance strategy that allows its customers to attain their own compliance to applicable laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and (e) ServiceNow's homogeneous environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible. The "Data Security Guide" contained within the "Subscription Service Guide" included with this response describes the measures ServiceNow takes to protect Customer Data when it resides in the ServiceNow cloud.
QTS	The QTS Information System Security Officer (ISSO) develops, disseminates, annually reviews and updates a formal, documented access control policy; System and Communications Protection and addresses the following: •Purpose and scope •Roles, responsibilities •Compliance QTS develops, disseminates, and annually reviews/updates a formal, documented security policy executive summary, SP Executive Summary - Information System Security Program Policies, which addresses: •management commitment •coordination among customer entities

	QTS cloud's Policies are maintained within a biometric secure office located in the Suwanee facility at 300 Satellite Blvd, Suwanee, GA 30024. It is disseminated to all individuals, including but not limited to employees, contractors, consultants, temporaries, and other personnel affiliated with third parties, who use any QTS Information Resource that is owned or leased by QTS. This policy is consistent with QTS's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. The previously mentioned artifacts are disseminated via a centralized secure document repository among all QTS cloud's personnel who have any service operations or service delivery role for QTS cloud's IaaS offerings system environments, and is to be individually or by group reviewed semi-annually, especially by any personnel who have administrative access. QTS can provide its Information Security Policies as required: • IT_POL_03_System_and_Communications_Protection_Policy (v1.2 – 1/17/14)	
SAP	Ariba	We are committed to the security and integrity of customer information. We utilize security measures to protect against the loss, misuse or alteration of the information under our control. To prevent unauthorized access, maintain data accuracy, and facilitate the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect within the solution.
	Fieldglass	Please see the Fieldglass Security and Hosting Overview provided in the Supplemental Information section of this response.
	Hanna	Communication between data centers is via VPN or MPLS; VPN is encrypted by default and MPLS can be encrypted as well. Internet facing customer systems are protected by perimeter protection systems using technologies such as web application firewall (WAF) or intrusion prevention systems (IPS). Perimeter protection systems operate by monitoring traffic and blocking attaches towards SAP HANA Enterprise Cloud customer systems.
	Hybris	Both IDS and IPS are included the SAP Hybris Commerce, Cloud Edition The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer.
	SuccessFactors	Technologies and measures used to help protect the security of customer data include: Redundant firewalls in a dedicated environment Network intrusion detection to help guard against attacks by monitoring all data center traffic around-the-clock and notifying operations and security teams in the event of an imminent threat Vulnerability scanning to proactively test internet-connected web servers by searching for weaknesses in the same way that a hacker would

		Penetration testing at least annually Security teams monitoring the infrastructure 24x7x365 Any security issues discovered are reported in real time to information security staff and IT management, entered into our ticketing system for follow-up investigation, and tracked to resolution. All actions taken to resolve the problem are documented, allowing all problems to be tracked to completion. We provide application level memory separation between each client instance as well as data level segmentation and separation with each customer's data residing in its own schema and table space at the database tier. The database tier provides isolation and security of data, and the use of application clustering provides availability, reliability and scalability. Each customer's data is maintained in a separate database schema with its own discrete set of tables, facilitating a high degree of data isolation thus preventing potential for data segmentation breaches Flexibility to backup individual customer table spaces without affecting adjacent customers Each schema has separate authentication credentials and assigned resource profile to restrict access rights and resource consumption
VMware	The VMWare Approach to Compliance Many organizations have initiatives to virtualize their Information Technology (IT) infrastructure, or to move to a Cloud Computing model. However, these initiatives are often complicated by the increasing number of regulatory compliance requirements, which require protection of data such as PCI, HIPAA, FISMA, DIACAP, FedRAMP, GLBA, and other State and Federal requirements. Organizations are increasingly concerned with the complexity, risk, and impact that a new technology can bring to their existing environments. VMware addresses these challenges by establishing a Compliance Reference Architecture Framework (RAF) that provides a consistent method for VMware, its partners, and customers to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure. We designed our security architecture using a defense-in-depth approach to implement multiple layers of security throughout the SaaS environment and to mitigate any potential attacks through multiple safeguards, including: • Access control mechanisms, firewalls, anti-virus/malware software, auditing mechanisms, network controls, maintaining defined configuration settings, etc. We perform regular internal scans to assess the vulnerability of our internal network.	
FireEye	All data is stored within locked and monitored cages in secure data centers. Customer data is restricted to a need to know basis. Data is logically tagged and virtually segregated in our cloud services. Access is managed and only given to those with need to know including internal employees and customers.	
VirtueStream	All data for this environment will remain in the United States. Customers can elect Intel's TxT technology to demonstrate geo-fencing of data to specific data centers. Virtustream data centers are physically accessible by designated employees and approved employees only. Virtustream employees who are assigned to the data center are issued a proximity card which is required to access the data center. Once inside, physical access to the data processing areas is further restricted to specific employees. Physical access to the data processing areas is protected by biometric locks on the doors. Data center personnel maintain a list of all approved personnel who have access to the data center offices and who have access to the data processing areas. Virtustream offers security solutions which customers can select to protect their data while in transit and at rest. Customers are responsible for the protection of their data within their customer	

	zone. Virtustream does not process, store, or disseminate customer data within the Virtustream-controlled management zone. Virtustream invokes a defense-in-depth model for monitoring the management zone with tools such as Splunk, Trend Micro, Fortinet, and Tenable. These tools are available for customers to select as a managed service.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

CA	APM	All personnel with access to client data undergo annual, mandatory security training and are covered under the CA Technologies NDA. Violations of security policies are grounds for termination. All access to data and other resources used to deliver the service are granted under the least principle.
	MAA	Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to MAA servers, and database administrators have access to database servers. Account access is reviewed periodically.
	CA Agile	All customer data is treated as confidental and as a policy we do not access customer data without explicit written consent. Access to systems containing customer data is restricted to our Operations Team according to our Elevated Permissions Policy.
	ASM	Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to ASM servers, and database administrators have access to database servers. Account access is reviewed periodically. All data on CA laptops are encrypted and a PIN is required to boot.
AODocs	The data stored in Google AppEngine are backed up every day. The application is hosted on Google Cloud Platform infrastructure and benefits from the network security.	
Virtru	See 'Virtru Security Policies and Procedures' and 'Virtru Privacy Policies and Procedures'	
Salesforce	Logical Access Control Salesforce provides contractual assurance to its customers that the data hosted in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances (such as a support issue) and only for a set amount of time chosen by customer. In such circumstances, we will access your org only with prior approval and subject to a Non-Disclosure Agreement (NDA). To protect against access through the application, Salesforce employees don't have access at the application level for any customers, unless the customer grants access through the “login as” feature. Access to the production environment infrastructure is restricted to a very limited number of full-time Salesforce employees required to manage the service. Salesforce's Technical Operations team and Release Managers have logical access to servers. These employees must authenticate to the production environment via a secure server (Secure Global Desktop) using 2 points of RSA two-factor authentication. This tool provides pixel data only to these administrators. Systems access is role-based and controlled and logged. DBAs do not have login access to customer's instances (org) and do not see customer data in an assembled manner. They manage the system in aggregate-performance tuning, allocating space, building indices, etc. The Oracle tables and rows in our infrastructure do not reflect the view of a single customer instance (org) since we are multi-tenant and the data is spread across multiple disk arrays.	

	Database administrator account activity is logged. These logs are sent to the security information and event management (SIEM) system. These database activities logs are reviewed for appropriateness by the Computer Security Incident Response Team (CSIRT) team on a regular basis. This log data is also available as a forensic audit trail to support CSIRT during incident investigations. A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.	
ServiceNow	ServiceNow applies the same data classification for all hosted customer data. ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data controller for all data placed into their instance. ServiceNow does not examine, inspect, monitor or analyze customers' data. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.	
QTS	The customer will be assigned one or more Org Administrators. All users will be configured with RSA AD two-factor Risk Based authentication as a requirement for cloud portal access.	
SAP	Ariba	We participate in the following national and international standards committees: WebTrust: (2001 - current) The Security, Availability, Processing Integrity and Confidentiality of our applications are based on the Trust Services Principles now incorporated into the SSAE16/ISAE 3000 SOC 2 standards SSAE16: (formerly SAS 70) certification: (Since 2011) ISAE 3402: (The International Standard on Assurance Engagements since 2014) every six months we undergo a rigorous ISAE 3402 audit by independent auditor PricewaterhouseCoopers (PwC) Payment Card Industry (PCI) Data Security Standard (DSS): (Since 2008) we have adopted and adhere to the PCI-DSS). PCI certification and compliance with the Visa USA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program Safe Harbor: (Since 2007) Current on the Safe Harbor list for ""Online Data"" for the ASN and Cloud Solutions/Services A firewall separates the Ariba corporate network from Ariba infrastructure computers. Therefore, unauthorized Ariba employees cannot access Ariba data from the Ariba corporate network infrastructure. Access is limited to specific roles or functions within Ariba Operations. Additionally, access is managed on an "exception" basis whereby personnel need clearance to be

		authorized. Access is time-limited, after which time re-authentication is required. Internally, we have deployed an active monitoring system tied back to Human Resources. Logical access management reports are rolled up monthly and are part of the monthly Privacy & Security board review. All logical access management is subject to review and audit under ISAE 3402 assurance every six months and annually under PCI DSS certification. Wireless technology is not allowed within the production operations infrastructure where customer data is received, processed and stored. All corporate laptops are whole disk encrypted. All approved portable devices are encrypted and have a phone home capability which allows them to be wiped remotely.
	Fieldglass	Fieldglass has the following categories for classifying information: Confidential - This is the information that Fieldglass and end users have a legal, regulatory and/or contractual obligation to protect or information that unauthorized disclosure, compromise, or destruction that results in severe damage, provides significant advantage to a competitor, or incurs serious financial impact to Fieldglass and/or our customers. Fieldglass will not disclose to a third party without signing a nondisclosure agreement requiring the third party to protect such information. Internal Use - This is information that, due to a technical or business sensitivity, requires special precautions to ensure the confidentiality and integrity of data by protecting it from unauthorized access, modification or deletion. This information is intended for use only within the company and must be limited to end users who are employed by Fieldglass or individuals that have a business requirement to access the data and have signed a non-disclosure agreement. Public - This information has been made available for public distribution through authorized company channels. Public information does not require special protection. It is information that can be disclosed to anyone without violating an individual's right of privacy. Knowledge of this information does not expose Fieldglass to financial loss, embarrassment, or jeopardize the security assets. Laptops Every Fieldglass laptop issued to employees and contractors have a DLP agent installed that cannot be modified. This agent detects whether customer data or the Fieldglass source code is being copied externally. Monthly access reviews are conducted by product and file share owners to ensure access is limited to a need-to-know basis. Privileged user account access is also monitored on a weekly basis.
	Hanna	SAP treats all customer data stored in cloud solutions from SAP as "Confidential" according to SAP's data classification standard. Personal Data is subject to strict security and legal requirements in the legislation of several countries, for example handling of Personal Data is regulated in the European Union (EU) Data Protection Directive and

		corresponding national laws. At SAP intercompany agreements exist, to ensure that these requirements are met in all SAP companies and branch offices throughout the world. Similar data protection agreements were executed with all subprocessors. Personal data must be classified as equally confidential regardless of whether it relates to employees, customers or third parties.
	Hybris	The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer.
	SuccessFactors	We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor.
VMware	VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of vCloud Air over which VMware have sole administrative level control. The goal of this process is to identify security incidents and respond to them proactively. This responsibility stops at any point where customers have control, permission, or access to modify any aspect of the service offering. The customer is responsible for the security of the networks over which they have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, and other such capabilities. Proactive Security Monitoring over Internet and Social Media (e.g. searching filesharing sites for customer data, seeding data with honey tokens) VMware security teams perform OSINT monitoring on the Internet for all VMware products and services. This includes harvesting data from search engines, le sharing, and social networking sites. This data is analyzed for keywords and other specific indicators. With regards to potential data leaks, the customer is solely responsible for protecting the security of his or her content, including any access provided to employees, customers or third parties. vCloud Air provides certain software and functionality to help protect content from unauthorized access such as firewalls, load balancers, and IPsec VPNs. Customers are encouraged to deploy additional security mechanisms similar to what exists in their current data center to address other security controls such as data encryption, intrusion detection, le integrity monitoring, and other such concerns relevant to the sector and regulatory requirements that apply to the specific business of a customer.	

FireEye	FireEye has mature and well documented security and privacy programs. The programs include third party certifications for SSAE 16 SOC 2, and FedRAMP certifications, Model clauses, Privacy and Security Standards among others. The data that FireEye receives is only in conjunction with the malware analysis. Our data protection standards includes prevention of exposure to unauthorized personnel and managing and reviewing all access to systems (not just for admin) quarterly or when employees have a role change. FireEye has standards for hardware and software such as gold images for all operating systems and hardened systems, these are managed and distributed centrally. It also includes supported and managed configurations of hardware and software on mobile devices and acceptable use policy for all FireEye resources.
VirtueStream	Customers are responsible for the protection and confidentiality of data within their application and/or system which resides on the Virtustream IaaS. Virtustream customers are logically separated via VLAN and VRF technologies which ensure that different customers' data is not accessible and cannot be altered. Customers are responsible for controlling access to their data. Virtustream does not have direct access to customer data within their customer zone. Virtustream employees who are assigned to IaaS must pass a Virtustream background investigation. In addition, Virtustream employees assigned to the IAAS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone. Virtustream offers an encryption at rest and encryption in transit managed service. This provides an additional level of protection for customer's data within their VLAN, All Virtustream employees with access to the IaaS are required to have hard drive encryption on their laptops. Virtustream performs quarterly privileged user access reviews.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits.
	MAA	CA MAA is certified for SOC 2 Type 1 Security Audit.
	CA Agile	N/A - we are working towards a NIST 800-53r4 certification but that is not yet complete.
	ASM	Rackspace datacenters annually undergo various certification including SOC 3 audits. The application currently does not hold a Soc 2 attestation.
Google	SOC 1 (SSAE 16) SOC 2 SOC 3 ISO 27001 ISO 27018 FedRAMP	
AODocs	AODocs is certified SOC2 Type 2	
Virtru	Vulnerability Scan and Penetration Testing by Cigital and FedRamp In Process sponsored by US Department of Interior	
Salesforce	Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties. The following audits and their frequencies are performed: ISO 27001 - Annually (3 year certification) PCI-DSS - Annually FedRAMP - Annually SOC 1 (SSAE16/ISAE 3402, previously SAS 70) - Twice a year SOC 2 & SOC 3 - Twice a year Copies of our SOC reports can be provided to your Agency upon request and under NDA.	

	Under NDA, your Agency can also be provided Salesforce's complete FedRAMP Authority to Operate (ATO) package, which contains the following security assessment documentation: 01 - Salesforce Government Cloud System Security Plan 02 - Salesforce Government Cloud System Security Plan - Tracked Changes 03 - Salesforce Government Cloud Attachment 1 - Control Tailoring Workbook (CTW) 04 - Salesforce Government Cloud Attachment 2 - Control Implementation Summary (CIS) 05 - Salesforce Government Cloud Attachment 3 - PTA and PIA 06 - Salesforce Government Cloud Attachment 4 - E-Authentication 07 - Salesforce Government Cloud Attachment 5 - FIPS 199 Categorization 08 - Salesforce Government Cloud Attachment 6 - User Guide - Customer Configurations 09 - Salesforce Government Cloud Attachment 7 - Hardware, Network, and Software System Inventory 10 - Salesforce Government Cloud Attachment 8 - Customer Responsibilities 11 - Salesforce Government Cloud Rules of Behavior - Ground Rules for Security Success 12 - Salesforce Government Cloud Disaster Recovery Plan 13 - Salesforce Government Cloud Incident Response Plan 14 - Salesforce Government Cloud Configuration Guide 15 - Salesforce Government Cloud Continuous Monitoring Plan 16 - Salesforce Government Cloud Security Assessment Plan 17 - Salesforce Government Cloud Security Assessment Report (SAR) 18 - Salesforce Government Cloud Table 4.1 SAR 19 - Salesforce Government Cloud Test Cases (SRTM) 20 - Salesforce Government Cloud POA&M	
ServiceNow	•ISO/IEC 27001:2013 BrightLine Certificate Number 1980700-4 (see supplemental information section for official certificate) •SSAE 16 SOC 1 Type 2 (available under NDA) •SSAE 16 SOC 2 Type 2 (available under NDA) •FedRAMP Compliant	
QTS	QTS maintains control mappings that include: • NIST 800-53/FedRAMP (Low/Moderate/High) • DOD IT RMF/DIACAP (MAC I/II/III Sensitive & Public) • HIPAA-HITECH-Omnibus • PCI-DSS • ISO/NATO • CNSS/ICD/DCID/NISPOM	
SAP	Ariba	As assurance collateral, we can provide the BITS SIG and CSA Cloud Service Provider Questionnaire, Our ISAE 3402 SOC 1 Type II, SOC 2 and SOC 3 reports as well as the Attestation of Compliance for PCI DSS are signed by our qualified security assessor and management.
	Fieldglass	Independent third-party auditors conduct annual audits for the following: • ISO 27001 • SSAE 16 SOC 1 and SOC 2
	Hanna	Please see response 8.6.1
	Hybris	
	SuccessFactors	We have various third party certifications including ISO 27001 and BS10012.

VMware	VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system (“ISMS”) as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization’s people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system (“ISMS”) as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization’s people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system (“ISMS”) as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization’s people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. vCloud Government Service (IaaS): FedRAMP Provisional Authority: VMware vCloud Government Service, provided by Carpathian, now has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a ""do once, use many times"" framework that can reduce government organizations' costs, time, and staff required to conduct redundant agency security assessments. U.S. government agencies can now leverage vCloud Government Service to meet the stringent security and privacy requirements of FedRAMP.
FireEye	We have SSAE 16 SOC 2 Type 2 certification for specific cloud services, and associated datacenters. FireEye currently has a FedRAMP ATO for ETP and are in process for full FedRAMP, and ISO 27001 certification.
VirtueStream	Security is the foundation of our business. Virtustream's xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain FedRAMP, FISMA Moderate, PCI-DSS, SSAE16/SOC2/SOC3, ISO 27001/9001/22301, HIPAA, NIST 800-53, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

CA	APM	CA has various log monitoring tools that help us keep track of live production systems in order to understand load vs. resource utilization vs. performance. CA along with AWS monitors the service and provides real time alerting when systems suddenly die, or when system loads or response times approach critical thresholds. Logs are kept for forensic examination and identification of trends in order to proactively ensure stability.
	MAA	CA MAA servers log all activity, and data retention is anywhere from 14 to 180 days depending on the component and volume of logs generated
	CA Agile	All systems are required to send logs to a centralized log server. At a minimum log data must contain timestamps, usernames, IP Addresses, and query parameters.
	ASM	ASM servers log all activity, and data retention is anywhere from 30 days to 1 year depending on the application and volume of logs generated.
Google	This is largely the responsibility of the customer. Google's obligations, as described in 8.6.4, are to ensure there is no unauthorized access of Customer data. Customers are responsibility for ensuring their end users use the service according to the Customer's acceptable use policies. During the onboard process, Customers will be assisted in the configuration controls that are included to enforce acceptable use and security policies and trained in how to maintain oversight on the ongoing usage of the services in scope.	
AODocs	AODocs does not manage the authentification. The authentification is managed by Google.	
Virtru	See 'Virtru Security Policies and Procedures'	
Salesforce	Salesforce Infrastructure Logs Salesforce internal infrastructure logs are collected by various monitoring tools for activities on the systems that host Salesforce, and include: Server access Network access Firewall management events Network intrusion detection systems traffic Cache Database File integrity Network device configuration Anti-virus detection Log events are correlated to generate alerts. Alerts are configured to notify the Technical Operations and Computer Security Incident Response Team (CSIRT) teams. Security alerts require acknowledgement and follow up, if appropriate by the CSIRT. Firewalls and IDS systems are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of (1) one year. NOTE: These logs are not available to customers. Customer Auditing Capabilities Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an	

	organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include: Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information. Login History - You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce. Field History Tracking - You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. Setup Audit Trail - Administrators can also view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to your organization's configuration. This trail can be downloaded into Excel or as a csv file. While the Login History and Setup Audit Trail are available for six months within Salesforce, audit trails can be downloaded and stored locally to meet longer audit log retention requirements. Detailed application logs can be used for forensics investigations by customers. These logs are stored for 12 months and are available for a fee. Event Monitoring (Additional License Option) In addition to Salesforce's core auditing capabilities, Salesforce also offers Event Monitoring as an additional license option. Your Agency can use event monitoring to discover how often and at what times your users are logging in to and out of your organization. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. Not only can your Agency now better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put your agency at risk. In addition, your Agency can also determine if an employee is unnecessarily downloading sensitive customer/citizen information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available. Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Force.com SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind: - In the unlikely case where no log files are generated for 24 hours, contact Salesforce. - Log data is read-only. You can't insert, update, or delete log data. - Use the EventType field to determine which files were generated for your organization - LogDate tracks usage activity for a 24-hour period, from 12:00 a.m. to 11:59 p.m. UTC time. - An event generates log data in real time. However, log files are generated the day after an event takes place, during nonpeak hours. Therefore, log file data is unavailable for at least one day after an event. - CreatedDate tracks when the log file was generated.

	- Log files, represented by the EventType field, are only generated if there is at least one event of that type for the day. If no events took place, the file won't be generated for that day - Log files are available based on CreatedDate for the last 30 days when organizations purchase User Event Monitoring or one day for Developer Edition organizations. Businesses desire certainty that their data is accurate, complete and reliable, enabling them to meet stringent industry regulations. With Field Audit Trail, customers can track changes at the field level for up to ten years and set different policies for each Salesforce object to ensure data is purged when no longer needed. Life sciences companies running clinical trials in Salesforce, for example, can now maintain a complete audit trail of patient data so they can safeguard the integrity of clinical trial results and comply with FDA regulations. - All event monitoring logs are exposed to the API through the EventLogFile object, however there is no access through the user interface. Event monitoring can be used with 28 different file types: Apex Callout, Apex Execution, Apex SOAP, Apex Trigger, API, Async Report, Bulk API, Change Set Operation, Content Distribution, Content Document Link, Content Transfer, Dashboard, Document Attachment Downloads, Login, Login As, Logout, MDAPI Operation, Multiblock Report, Package Install, Report, Report Export, REST API, Salesforce1, Adoption (UI Tracking), Sandbox, Sites, Time-Based Workflow, URI, Visualforce. Event Monitoring Transaction Security Transaction Security policies give your Agency a way to look through events in your organization and specify actions to take when certain combinations occur. A transaction security policy consists of events, notifications, and actions. Transaction Security monitors events according to the policies that your Agency sets up. When a policy is triggered, you can receive a notification and have an optional action taken. For example, suppose that you activate a policy to limit the number of concurrent sessions per user to three. A user with three login sessions tries to create a fourth session. Your Agency can require a user to end one of their existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered.
ServiceNow	The ServiceNow application writes detailed log information that is stored in tables within a customer's instance. As this is customer data in a customer's instance, ServiceNow does not attempt to monitor or view this data unless specifically requested by a customer. As a result the customer is responsible for monitoring the contents of these logs files. The log data is protected in the same manner as all other customer data. Event logs can also be configured to feed into a customer's environment via ServiceNow's Syslog probe allowing the logs to be stored within the customer's environment in a syslog repository or SIEM and retained according to the customer's requirements. ServiceNow's application logging includes verbose transaction logs, these logs are retained within the instance for 30 days. Event logs are stored for seven days and audit histories are retained indefinitely in the instance. Transaction logs represent every click, view, and system event that occurs in an instance and as a result, will grow very large, quickly. They provide a level of detail that is frequently used for troubleshooting issues with an instance. They can also provide detailed intelligence on the behaviors within an instance. These logs can be downloaded to customers' environments, if they need to be retained for longer than 30 days. The event logs on the other hand are less granular; they will include the creation of an incident, or deletion of problem, or any one of the 250 standard events. They may also contain customer

	created events. There are a number of security events as well, including successful login, failed login, security privilege escalation, and viewing of a table. These events can either be monitored manually, generate an Incident based on a parameter or when metric is reached; such as failed logins per minute. The final aspect of logging is the audit history. Audit history may be turned on for any particular table or field. The audit log table then maintains a record of who made changes when to a table or field and what they changed.
QTS	All account activities are logged including account creation, modification, disabling and termination. Logs are monitored and notifications are sent for abnormal activity. Splunk Enterprise is used as the centralized audit log monitoring tool to centrally collect, analyze and reduce the amount of audit logs. As referenced in IT_PRO_07_Audit_and_Accountability_Procedure (v1.0 – 1/20/14), on-site network and security operations monitoring coverage and audit management process; to include analysis, reporting, and alerting into a central repository provided by a highly available Splunk logging service. Splunk logging service supports QTS cloud information systems for organizational–wide situation awareness. Splunk provides built-in capabilities to filter, normalize, and correlate the large amounts of data produced by QTS cloud, and then allows QTS's support staff to use Splunk's built-in capabilities to data mine, log mine, and run pre-developed and ad-hoc reports against the result sets obtained during the data and log mining sessions. Logs are centrally correlated and reviewed from devices across QTS cloud Hosting Environment by QTS's Systems Engineer or designee. Specific report categories include: •Authentication and Authorization Reports • Systems and Data Change Reports •Network Activity Reports •Resource Access Reports •Malware Activity Reports •Failure and Critical Error Reports • Vulnerability Correlations Reports •Anti-Port Correlations Reports •Watch List Correlations Reports
VMware	VMware IaaS Services In accordance with our ISO and SOC commitments, change-related activity, including administrative actions, performed on the management infrastructure layers supporting vCloud Air are monitored and logged to a centralized logging server for a minimum of 1 year. Infrastructure logging is in place for customer interactions with the vCloud Air management and administrative consoles. These logs are only for the management and administrative interfaces. These are not in place for monitoring of individual customer VMs installed within the customer tenant org. Limited logging and activity reporting are available from customer tenant environments, with more detailed reporting, auditing and logging capabilities introduced Q4-2014. VMware AirWatch To enable user accountability, we have full auditing capabilities on all environments in the AirWatch Cloud. Customers can use the built-in event log, customizable dashboards, integrated reporting engine and AirWatch Hub to audit the web console and end-user actions. For the SaaS environment logs, our Information Security Team helps ensure that systems generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
FireEye	FireEye auditing and log review procedures are based on industry best practices and in accordance with regulatory, statutory, contractual and business requirements. Detailed audit

	records (User ID, date, time, type of event, successful/unsuccessful attempts or access secured files and protect the contents of audit trails against unauthorized access, modification or deletion.
VirtueStream	Virtustream offers logging as a managed service to customers as optional solution. The types of services and devices are specified by the customer and a monthly report is delivered to the customer.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

CA	APM	Users of the Portal are divided into two types: Internal users (for publishers of the API) and External users (for developers). There are a number of pre-defined roles for both Internal and External users that inherit functionality in a hierarchical manner. Portal has RBAC built in that allows you to grant access to different functionality for different users. For example, you can assign a user to role that only allows them access to update content, or access apps but not create them.
	MAA	CA utilizes IaaS vendor to host the service with strict access controls in place. CA SaaS InfoSec team manages users and their associations with groups within LDAP Directory and conducts periodic access reviews to conform to governance requirements.
	CA Agile	Our databases are shared but logically segregated. We ensure logical security of access to customer data by implementing access restrictions between subscriptions and roles within those subscriptions to assure adequate segregation of data. There is a plugin available in the unlimited edition that allows the administrator to limit access to the application based on IP address.
	ASM	Only Public Status Page (PSP) data is stored in the cloud, and PSP web pages are accessible by anyone. PSP data is only sent to the cloud if the customer enables this feature, and they can decide which data is made public.
Google	If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.	
AODocs	The AODocs-specific data stored in the Google App Engine Datastore relies on a built-in multi-tenancy feature named "namespace", which define virtual "silos" within the AODocs database. Each customer is assigned a specific namespace (which is in fact the customer's primary Google Apps domain name), and all the customer's data is stored within this namespace.	
Virtru	Key material is encrypted prior to storage, and those keys are backed by HSM. Decryption occurs only for authenticated users	
Salesforce	The multitenant architecture and secure logical controls address separation of customer data. There are no dedicated servers used for individual customers. The Salesforce Services infrastructure is divided into a modular architecture based on "Instance". Each Instance is capable	

	of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer's org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers.	
ServiceNow	ServiceNow includes built in Role Based Access Control (RBAC) that is based on users, groups and roles. The entitlements granted to users are built from fine grained Access Control Lists (ACLs). ACLs can be built from individual entitlements that include read, write, create, execute and delete as well as a number of other individual attributes. The attributes that are available also vary, depending on the type of object being secured. Customers have full control of the entitlements granted to each of their users and integration with customer side directory service is possible through the use of users, groups and group memberships.	
SAP	Ariba	Within our solution, specific logging takes place that is viewable by the customer administrator or their designee. Audit logs produced through use of the solution are considered customer data and are maintained within the customer's instance of the database. These logs are retained so long as the customer has an active contract with us. As a user control consideration, customers are responsible for monitoring the proper entry of data to the solution and reviewing reports generated by the system.
	Fieldglass	The Fieldglass Audit Trail tracks a date/time stamp for each user as they log in and out of the application. Likewise, Fieldglass tracks a date/time stamp and owner of every transaction that is created, submitted and approved through the application. Similarly, actions that occur within the reporting tool are also tracked, including when reports are created and run and by whom. The audit trail log is visible by the State of Utah program office. Audit trail reports can be created with Fieldglass' ad hoc reporting.
	Hanna	SAP has Security Information and Event Management systems (SIEM) for analysis, reporting and alerting. All critical systems and infrastructure components within the SAP Cloud need to log relevant data, which is stored for a minimum of six (6) months. This is ensured via the security configuration compliance checks and event monitoring. General security monitoring is performed 24x7 for all activities. Resulting warnings and alerts are processed via ticketing system and critical events are handled according to the Incident Management Process.
	Hybris	Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. hybris utilizes technologies from leading security firms for Log Management and File Integrity Management.
	SuccessFactors	The application logs the following for every transaction: Event/transaction Time, Transaction ID, Event/transaction Type, Event/transaction Status (Result of the event; if failure, includes reason), Object Attributes (Describes the object affected by the event), Originator User ID (ID of the user who initiated the event or action), Subject ID, Process User ID, Account Number, Transaction Specific Elements. The application audits changes to the major components. Examples of this are goal auditing and document auditing. The audit trail includes who made the

		change, the date of the change and the ability to see the data as it existed at that point in time. The data in the audit log can be viewed with appropriate permissions. We also provide an optional Audit Framework for additional audit logging capabilities. All audit logs within the application are accessible only by customers. Therefore, the review of application audit logs as well as retention periods for the application audit logs are the customer's responsibility, and can be determined as per requirements. To detect unauthorized information processing activities, systems are monitored and all information security events are recorded. Operator logs and fault logging are used to information system problems are identified. We comply with all relevant legal requirements applicable to its monitoring and logging activities. All system logs are created with "write-once" technology so that they cannot be altered or overwritten. All system logs are maintained for a minimum of 90 days on-line and a minimum of 13 months near-line. Inter host communications are secured by multiple layers of defense including segmented separate VLANS, restricted protocol sharing, multiple levels of stateful firewalls, HOST and NETWORK IDS/IPS and constant vigilant monitoring and testing. In addition, our Operations Team maintains detailed system logs. Our internal system logs successful and unsuccessful requests for access, and our team monitors all system logs for any errors or unusual activity. Activities are logged and reviewed by various mechanisms such as: RSA, SysLog, NIDS, HIDS, OSSIM and database logging. The system logs are not made available to customers but are used to monitor the health of the application and facilitate a high level of performance. Alerts are responded to immediately and logs are analyzed daily for any issues or anomalies. The system level logs are written to servers in the data center then copied to our operations team on an as needed basis. Various logging mechanisms are used to monitor database administration activities. Logging mechanisms include: syslog, alert log and database auditing for the privileged role SYSDBA. All activities are logged under the SYSDBA role which including: start-up and shutdown of the data base, configuration changes to init.ora and also any queries/data extraction. We would be able to identify dba activities by manual review of the logs and database auditing to detect if client data querying has occurred. All audit logs are created with "write-once" technology so that they cannot be altered or overwritten. Controls aim to protect against unauthorized changes and operational problems with the logging facility including: Alterations to the message types that are recorded. Log files being edited or deleted. Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
VMware	The vCloud Air Terms of Service and Data Privacy Addendum's establish the line of demarcation between the responsibility of VMware and the customer as it pertains to data protection. In addition, security whitepapers are made available to customers to further illustrate these points or to establish transparency regarding the separation of responsibility between VMware and the customer for compliance programs such as HIPAA or PCI. Subscribers are able to use a VPN connection at multiple layers to maintain data security. For traffic in motion, VPNs can be created for a particular application and also for an entire virtual data	

	center. A site-to-site IPsec-VPN can also be established to securely tunnel the entire virtual data center back to the private data center. For data ""at rest"", subscribers are provided a role-based access control, whereby specified users are not exposed to the entire infrastructure and can be limited to a single or multiple virtual data centers. Further details of the controls in place to limit exposure of these groups to customer data is documented within the ATA 101 and SOC reports, available under NDA. vCloud Air has logically separated networks that restrict Tenant access to only their own private networks. The vCloud Hybrid Service has two offerings: The Dedicated Cloud option provides physically isolated and reserved compute resources from all other vCloud Hybrid Service tenants, as well as a private cloud instance. The Virtual Private Cloud option has a multitenant compute resource mode. Both services have logically isolated networking and storage that ensures secure resource separation. Customers have complete control over the file systems and databases they deploy within the service. Access is technologically enforced and employees are only authorized the level of access to information assets that is required to meet an approved business need or perform prescribed job responsibilities. • Administrative access is limited to only those users that explicitly require privileged access. Customers do not have direct access to the SaaS environment; rather, customers administer the solution via the Web console.
FireEye	Each of the FireEye offerings include strong access controls including role-based access. Only properly authorized individuals on a need to know basis are granted access to data.
VirtueStream	Virtustream does not have access to customer hosted data. Customers control access to their application or system which sits upon the IaaS. Customer would need to create the user in their own Active Directory to allow access by named users of Virtustream for specific system.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

CA	APM	CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant parties for notification. All security incidents will be investigated and triaged to understand where the vulnerability exists. Software vulnerabilities will be investigated by CA engineering teams; other vulnerabilities will be addressed by the SaaS Ops team in conjunction with AWS. Affected customers will be notified and given a remediation plan
	MAA	Clients are notified via email of any security incident that resulted in a data breach for that client promptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be setup upon request.
	CA Agile	We have a defined Incident Handling Guide which outlines the process and responsibilities during breach investigation. Clients are notified via email of any security incident that resulted in a data breach for that client promoptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be seutp upon request.
	ASM	Clients are notified via email of any security incident that resulted in a data breach for that client promptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be setup upon request.
Google	Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-	

	designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multifactor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever step foot in one of our data centers. Google operates a global, multi-tenant environment running the world's second largest IP data network providing customers with a low latency, high performing platform that runs 24x7. Hard Disks are assets that are tracked throughout its lifecycle at Google from arrival to final destruction. These disks are component parts that Google uses to build its own servers from other component parts including motherboards and a harden, highly customized version of Linux. Google uses a proprietary storage and processing mechanism that isolates processing of data in chrooted jails within a physical server. Access permissions restrict the ability for processes to interact between jails. In addition, tenant data is striped in chunks across many different drives with each chunk having its own access control list. This helps ensure that data is logically isolated between customers in storage and during processing. In addition to the inherent processing and storage mechanisms described above, Google's security controls including least privilege rights, logging and auditing have been implemented consistent with FedRAMP requirements
AODocs	Altirnao can use multiple notification channels to communicate incident updates to its customers: the AODocs status page (https://status.aodocs.com) provide status updates on all the AODocs services the AODocs customer mailing list, which can be used to send emails to the technical contacts of all AODocs customers the AODocs support platform, i.e. ZenDesk, which can be used to communicate with specific customers who have opened tickets.
Salesforce	Incident Response If negotiated into a final contract, Salesforce can promptly notify the Customer in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com. Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Government customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com. Salesforce will respond in accordance with the incident response process described above. Our incident response plan/process was created in accordance with FedRAMP moderate control requirements which include incident response requirements derived from NIST SP 800-53, NIST SP 800-61, and the FedRAMP Incident Communications Procedure.
ServiceNow	Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow shall report to Customer the unauthorized acquisition, access, use, disclosure or destruction of Customer Data (a "Breach") promptly following determination by ServiceNow that a Breach occurred. The initial report shall be made to Customer security contact(s) designated in

	ServiceNow's customer support portal. ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach. See the "Data Security Guide" contained within the "Subscription Service Guide" included with this response for additional information.	
QTS	Security Incident handling capability and process is outlined in the following Incident Response related procedures and plans: •FED_PLN_01_Incident_Response_Plan (v1.2 – 4/09/14) •IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 – 1/17/14) •IT_PRO_18_ISSO_IRT_Incident_Response_Guidelines_Procedure (v1.2 – 12/11/13) •OPS_PRO_77_OSC_New_Incident_Creation_Procedure (v1.0 -1/23/14) •OPS_PRO_62_Best_Practices_for_Incident_Handling_Procedure (v1.0 – 12/10/13) •OPS_PRO_72_BPG_OSC_Working_and_Resolving_Incidents_Procedure (v1.0 – 1/22/14) •OPS_PRO_84_BPG_OSC_Major_Incident_Management_Procedure (v1.0 – 1/27/14) As outlined in QTS's IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 -1/17/14) and FED_PLN_01_Incident_Response_Plan (v1.2 – 4/09/14): •Preparation activities, to include: -Ensuring the security of systems, networks, and applications through periodic risk assessments of systems and applications to prevent incidents. -Increasing user awareness of policies and procedures regarding appropriate use of networks, systems, and applications. -Sharing applicable lessons learned from previous incidents (particularly those involving malicious code and violations of acceptable use policies) with users so they can see how their actions could affect the organization. -Training Federal Cloud System Administrators to maintain their networks, systems, and applications in accordance with the organization's security standards. •Detecting activities, to include: -As referenced in QTS's IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 -1/17/14), review and analysis of continuous monitoring tools and related log file(s). -3rd Party monitoring services (Alert Logic): help detect and alert on changes in certain resources (e.g., Web pages) or publicly accessible services, such as Web, Domain Name System (DNS) and FTP servers. -File Integrity Checking Software: help detect any changes to important files caused by incident -IDS are set up for scanning and detection. Detection is achieved either by log analysis, packet capture review or image acquisition and analysis. •Analysis Activities, to include: -QTS IR Team is activated and incident identification is performed -Continued and targeted review and analysis of continuous monitoring tools, related log file, and corresponding applications would be performed. -If an Incident Response Team is required then at least one member of IT Security along with one or more members of QTS's IT Operations organization responsible for the affected system, as well as any necessary representatives from Network	
SAP	Ariba	We can provide a general overview but our full documentation is confidential. All of our security processes and procedures are audited by a third party every six months for ISAE 3402 assurance. We also hold PCI DSS certification. The

		intent of the following is to describe in a broad manner the actions we take in regard to security incidents, their management, tracking and communications in regard to internal policies and procedures. We have an established security incident plan based on internally-developed policies and procedures where documented results of all security incidents occurring during the six month audit period are reviewed and evaluated against the Trust Services Principles of ISAE 3402 and the PCI DSS standards as appropriate. Upon notification of a security incident, a documentation trail is begun by the InfoSec department and an internal ticket is created as the record of reference. The lead security manger calls a meeting including all personnel required to contain and reduce risk and impact appropriate to the nature of the incident. Tasks are assigned with milestones to be met to validate and determine extent of the incident. Communication is made to the Privacy & Security Board to alert principal membership and foster internal cooperation and awareness. An appropriate communication channel to affected customer(s) is determined based on how we were notified of the incident, i.e. from a customer, from an internal report or from a third party report. Communication is made to affected customer(s) to include the nature of the incident, actions taken to contain the incident and potential effects of actions if any, in regard to sustained business process and availability of the system. Any workarounds or hot fixes necessary in the solutions are communicated and scheduled reporting to the customer(s) is established with an identified single point of contact within our company. Based on the nature of the incident, if required, legal counsel present at initial risk & impact meeting, will assist in communicating with law enforcement contacts. The customer is kept informed of the milestones met and at scheduled intervals until the incident is fully contained and no further risk and impact perceived. All incidents are required to be internally managed by InfoSec to include tracking and review on a weekly basis and evaluation of the actions taken in regard to our security concept. All incident reports are presented to and reviewed by the Privacy & Security Board and are formally closed with discussion and evaluation to determine what actions can be taken to prevent similar incidents. Depending on the nature of the incident and impact to customer(s), security incidents are not formally closed by the board until all affected customers are made aware of the incident and appropriate measures to remediate the initial threat are formally communicated.
	Fieldglass	Fieldglass' security team is responsible for managing security incidents and all communication is conducted via the respective account managers to ensure timeliness. The process is defined within the Incident Response Management Standard. Customers are notified of an incident within 48 hours.
	Hanna	SAP will notify via defined communication channels within 36 hours of a confirmed data security breaches to the affected customers. The report will detail the following information: • Details relating to the security incident that has occurred, known at the time of notification. • IT infrastructure and/or application affected by the security incident. • Overview of the performed mitigation actions to restore the security, documented within the incident report form. • All further applicable requirements by country regulations "on obligation to notify" will be met.

	Hybris	Upon a breach that directly affects a customer's environment, hybris would notify the customer as quickly as reasonably possible. Furthermore, hybris follows its information security incident management policy as well as Visa's standard process for responding to a breach. The policy includes procedures such as disclosure of sensitive information, disclosure of system vulnerability, public release of vulnerability information, system vulnerability exploitation as well as incident reporting, contacting of law enforcement and forensic investigation.
	SuccessFactors	We have a comprehensive and approved Incident Management Policy and process. Upon the occurrence of a security incident, initial communication is distributed to the appropriate individuals and an escalation process is followed. Upon becoming aware of the incident, measures are promptly taken by the team to resolve the situation. All affected customers should be informed within at most 36 hours of confirming a potential breach in the privacy of their data. Following incident resolution, follow-up is required to ensure that the incident has been resolved effectively and that the threat is no longer present. We are aligned with ISO 27k standards for event and incident management and have formal incident management policies and processes in place. These policies and procedures are tested in the ISO 27k and SOC 2 audits.
VMware	VMware IaaS Services If VMware determines that there has been unauthorized access to, or use or disclosure of, Your Content, or other incident VMware will use commercially reasonable efforts to notify You, taking into account any applicable law, regulation, or governmental request. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Hybrid Service servers, storage, applications, and network devices. Documented escalation procedures and a ticketing system are in place to guide employees in identifying, reporting, and responding to system availability issues and related security incidents. This includes an incident response policy to determine severity of an incident and a breach notification process. All alerting and monitoring at the guest OS\VM level is the responsibility of the customer. In the event of a data breach customers will be notified by VMware vCloud Air Global Support Services via their preferred contact means. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices. Notification timeframes are agreed upon between VMware and the customer in standard agreements and contracts. Incidents are handled on a case-by-case basis, but typically occur between 24-48 hours after a breach has been confirmed. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices.	
FireEye	FireEye has a developed documented process for reporting client notification for regulatory, legal and contractual issues once a breach has been confirmed.	
VirtueStream	Virtustream shall contact customers in accordance with Service Level Agreements (SLA) and contractual obligations. There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security	

	Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'. The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement. The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS. The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan. As the incident progresses and has more impact (i.e. severity level increases), the escalation process will be used to engage appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits.
	MAA	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
	CA Agile	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security

		officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
	ASM	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
AODocs	N/A because all our data is hosted on the Google Cloud Platform infrastructure.	
Virtru	We require 2 Factor and Private Keys to authenticate and Virtrual Private Clouds for purposes of Inter-machine communication	
Salesforce	A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.	
ServiceNow	ServiceNow's architecture is built on a ServiceNow fully owned operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The ServiceNow private cloud operates out of colocation data centers that provide robust physical and environmental controls, with ServiceNow staff exclusively providing the logical management. Access to the private cloud where customer data is hosted is only granted to ServiceNow staff based on their roles and job requirements. ServiceNow does not outsource any function that would give a third party access to customer data. ServiceNow's private cloud is a highly standardized environment from the identically configured cages in the data centers through to the consistent logical infrastructure. This private cloud is home to just ServiceNow, limiting the private cloud's footprint to only those technologies required to support this service. This allows for highly restricted networking rule sets regarding ingress and egress requirements and facilitates the ability for hardened systems, only allowing for the small number of necessary services, protocols and ports to be enabled. A ServiceNow instance represents an isolated logical environment consisting of application nodes in the web application tier and a dedicated database. Each customer will receive at least two instances, a production High Availability (HA) instance and a sub-production instance without HA. Each instance is accessed via a unique Domain name in the form of 'customername.service-now.com' (for a production instance) and 'customername-dev.service-now.com' as a sub-production example.	

	There is no comingling of any customer data between instances and there is no single shared multi-tenant databases, with data from multiple customers stored therein.	
QTS	QTS cloud employs security controls as needed to protect the confidentiality and integrity of the information being transmitted by utilizing Cisco AnyConnect VPN Client with SSL (TLS and DTLS) and IPSec (Internet Key Exchange Version 2 [IKEv2]). DTLS provides an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCPbased application access, TLS (HTTP over TLS/SSL) ensures availability of network connectivity through locked down environments, including those using web proxy servers. IPSec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPSec and complies with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance. The QTS Federal Cloud Infrastructure (QTS cloud) is divided into two separate, isolated firewalled environments, each having its own security boundaries, which are physically and logically separated. These are the QTS cloud Hypervisor Management Layer and the QTS cloud Service Delivery Layer. QTS cloud's Hypervisor Management Layer management is made available through dynamic FIPS 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances. Once fully authenticated, only a limited RDP session to the physical bastion host (which is also protected by the RSA SecurID multi-factor authentication security appliances) via jump domains is allowed, which prevents the presentation of information systems management related functionality at an interface for general users. QTS cloud's Service Delivery Layer management is also made available through FIPS 140-2 validated L2TP/IPSEC or SSL 3.0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances. Connection to the QTS cloud Service Delivery Layer is only available through dedicated site-to-site 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels or Trusted Internet Connection (TIC) monitored dedicated datelines to federal customer datacenters, which prevents the presentation of information systems management related functionality at an interface for general users. QTS cloud's Hypervisor Management Layer management is made available through dynamic FIPS 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances.	
SAP	Ariba	The Cisco Secure ASA5555 Firewall is a dedicated firewall appliance that delivers strong security and performance and creates almost no network performance impact. The product enforces secure access between an internal network and Internet, extranet, or intranet links. Ariba uses Cisco Secure ASA5555 Firewall hardware and Cisco Router access lists to control the traffic to and from the Internet, between Ariba Corporate and the Ariba system, and between servers in Ariba. The firewall servers are configured for Fail-Over/Hot Standby Setup. Additionally, Ariba uses internally developed Ariba SafeGuard software to protect customer data from unauthorized Ariba Corporate users, allowing only Ariba Operations personnel access for limited periods of time. Specifically, firewall servers are used in each level of data communication within Ariba: Between the Internet and web servers Between the web servers and the application servers Between the application servers and the database servers

		These ASA5555 Firewall servers allow Ariba Operations to rigorously protect Ariba from unauthorized access, providing full firewall security protection. The Equinix Data Center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of the center are monitored and recorded using CCTV, and all access points are controlled. The Data Center is staffed with 24-hour security officers. Visitors are screened upon entry to verify identity, and escorted to appropriate locations. Access history is recorded for audit purposes.
	Fieldglass	Please see the Fieldglass Security and Hosting Overview provided in the Supplemental Information section of this response.
	Hanna	The fundamental security architecture of the SAP Cloud infrastructure is the principal of a private cloud. Customers receive an isolated, logical grouping of several virtual machines and physical systems in dedicated customer private networks. Customer private networks are segregated from each other using virtual local area networks (VLAN) technology. Customer systems are deployed in the respective customer private network. Though customers are only able to view or access systems within their assigned customer private network. Design of customer private networks has to be defined in a workshop between SAP and the customer. Multiple customer private networks might be required to separate different tier levels or to implement customer data flow restrictions. SAP HANA Enterprise Cloud administrative tasks will be done using management networks. Administrative access to the management networks from the SAP internal networks is only possible using dedicated jump hosts with strong authentication. Security of the SAP internal network including SAP end user equipment is ensured using solutions like network admission control, Intrusion Prevention Systems, network filtering, strong authentication for remote access, internet content filtering, anti-virus scanner.
	SuccessFactors	We serve our customers and end users from secure data centers around the world. Physical security features at these facilities include a 24x7x365 manned security station and biometric and man-trap access controls. The systems at these facilities are protected by firewalls and encryption technology. Operational redundancy features include redundant power, on-site backup generators, and environmental controls and monitoring. We employ a wide range of security features, including two factor authentication, data encryption, encoded session identifications and passwords. Our hosting providers conduct regular security audits of our infrastructure. We also employ outside vendors for 24x7x365 managed network security and monitoring. Every page we serve is delivered encrypted to the end user via a Transport Layer Security or TLS. We also use encryption technology in our storage systems. We continuously monitor the performance of our cloud offerings using a variety of automated tools. The architecture is designed with built-in redundancy for key components. We load balance at each tier in the network infrastructure. We also designed our application server clusters so that

		servers can fail without interrupting the user experience, and our database servers are clustered for failover. We regularly back up customer data. We have implemented a multi-tiered architecture leveraging a strategy of "defense in depth" with 6 tiers of virtual networks (VLAN) for separation at each delivery layer. Network traffic is logged and monitored with live monitoring through an Intrusion Detection System (NIDS), and controlled through a series of switches and routers whereas data must pass through each tier in order to get to the next tier. In addition to Physical (site) security, the logical network stratification includes the following: Tier 1 (External VLAN/firewall) - The first tier consists of the external network and perimeter firewalls. These provide an initial layer of defense and protect the following layers from unauthorized access. Note that port 443 (HTTPS for web traffic) is the only port open. Tier 2 (Internal VLAN/firewall) - A de-militarized zone (DMZ) exists with load balancers. The DMZ provides a second line of defense while the load balancers are the first layer of scalability for the service delivery. The DMZ functions as a ""neutral zone"" between the network and the outside public network. Tier 3 (Web VLAN) - The Web tier presents the User Interface to the application, and separates the application, reporting and utility servers from the other tiers. Tier 4 (Application VLAN) - The Application tier contains the business logic and transaction servers, and is managed through clustered, high availability (HA) servers. Pre-configured as "Pods", additional servers can be added as needed to provide scalability and performance. Tier 5 (Database VLAN) - The database tier is protected by an additional set of perimeter firewalls. The database processing is executed on database servers leveraging a multi-tenant, fully qualified database schema. Tier 6 (Storage VLAN) - Data is persisted to disks with include a Storage Area Network (SAN). Prior to store, data is encrypted by way of data appliance with AES-256 bit encryption.
VMware	VMware IaaS Services At the tenant level firewall services are provided via the vCloud Networking & Security Edge Gateways for customers to configure and maintain. Firewall policies can be used to restrict and manage public/Internet-based traffic and create DMZ zones for multi-tier applications. Firewall policies can also be used to configure access policies between internal IP networks and VxLAN segments. Stateful inspection firewalling can be applied on the external interface of the vCNS Edge Gateway. VMware architects, provisions, monitors and manages the vCloud Hybrid Service infrastructure and surrounding components. As described in the AT 101 (ISO 27001) report, access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The details of this control are not disclosed publicly. VMware AirWatch We implement multiple security measures to protect hosted servers, including physical and logical controls. Due to FOIA requirements and the competitive EMM marketplace, we cannot provide specific architecture details at this time.	

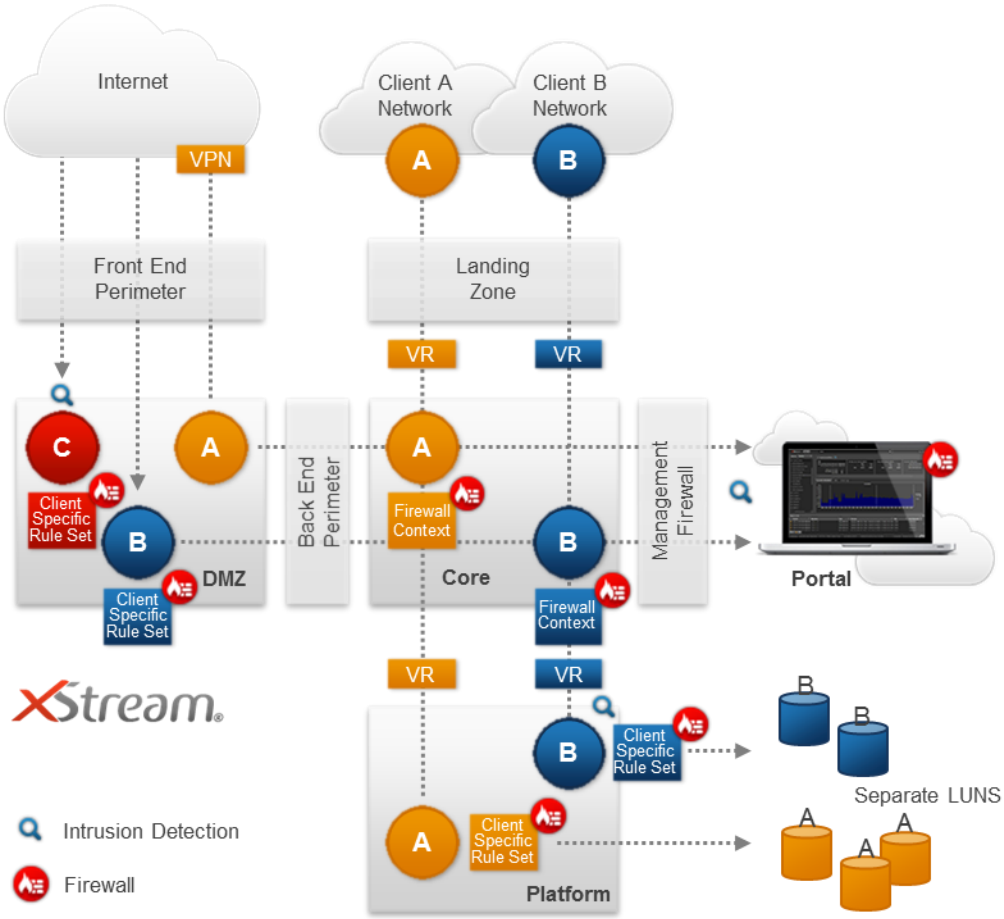
FireEye	High-level architecture diagrams following industry best practices utilizing both virtual and physical controls are available and contained in the SOC 2 report.
VirtueStream	Virtustream utilized a virtual local area network (VLAN) and virtual route forwarding (VRF) to logically segregate all customers in the IaaS environment. Every customer chooses their own IP Address range, as there is no ability to overlap IP Addresses between customers. In addition, every customer is logically separated with Firewall Context with their own rule, where by default everything is denied except specific rule.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

CA	APM	Only SaaS is provided, network diagram can be provided upon signing NDA
	MAA	Only SaaS is provided, network diagram can be provided upon signing NDA
	CA Agile	These can be provided when a NDA is in place.
	ASM	Only SaaS is provided, network diagram can be provided upon signing NDA
Salesforce	Salesforce offers market leading PaaS and market leading SaaS solutions. Salesforce does not provide IaaS as a direct service offering to our customers, it is an underlying part of our PaaS and SaaS offerings. The Salesforce Platform is built for cloud computing, with multitenancy inherent in its design. To meet the high demands of its large user population, Force.com's foundation is a metadata-driven software architecture that enables multi-tenant applications. Force.com combines several different persistence technologies, including a custom-designed relational database schema, which are innately designed for clouds and multitenancy—no virtualization required. Force.com's core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Force.com's well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others. Every logical database object that Force.com exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Force.com's Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Force.com does not create an actual table in a database or compile any code. Instead, Force.com simply stores metadata that the system's engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that's required is a simple non-blocking update to the corresponding metadata. Because metadata is a key ingredient of Force.com applications, the system's runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Force.com uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.	

	The multitenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on "instances". Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's Salesforce instance from being compromised. This functionality has been designed and undergoes robust testing through an on-going process by both Salesforce and its customers.	
QTS	The QTS cloud makes use of unique managed service provider architecture layer(s). Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the QTS cloud that are defined in its System Security Plan, and are not leveraged by any other Provisional Authorizations, are: Infrastructure as a Service (IaaS). Note: Please refer to NIST SP 800-145 for information on cloud computing architecture models.	
SAP	Ariba	Ariba recognizes that security is a critical component of effective electronic commerce architecture and takes necessary security measures to protect any information passed between buyers and suppliers. Ariba implements security using a variety of hardware, software, and procedural best practices. Full details about our security mechanisms and procedures are available in Chapter 3 of the Ariba Cloud Technical Infrastructure Whitepaper.
	Hanna	N/A, HANA Enterprise Cloud is a private managed cloud
	SuccessFactors	We understand the critical importance of information protection and recognize the contribution that information security makes to an organization's strategic initiatives and overall risk management. We have implemented security controls and practices designed to protect the confidentiality, integrity, and availability of customer information. We continually work to strengthen and improve those security controls and practices as well. The current best practices associated with information security involve a layered approach, what the industry calls "defense in depth." Regardless of the software delivery model, security cannot be implemented at a single "make or break" point. For a SaaS provider to facilitate data security for sensitive information, it must have a comprehensive, multifaceted security program in place. We take a holistic approach to information security, implementing a multilayered defense at all the touch points in the information flow—both the physical and logical, applied across the database, middleware, application, and network and communication layers—to offer complete data privacy, transparency, and audit controls.
VMware	Compliance Reference Architecture Framework (RAF) that provides a consistent method for VMware, its partners, and customers to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure. This includes: Product Applicability Guide (PAG), Architecture Design Guide (ADG), and a Validated Reference Architecture (VRA).	
FireEye	High-level architecture diagrams following industry best practices utilizing both virtual and physical controls are available and contained in the SOC 2 Type 2 report.	
VirtueStream	Virtustream Cloud Platform Security (for the Infrastructure-as-a-Service environment) is designed, built, and operated to provide highest level of infrastructure security available. **Proposed State of Utah Security Architecture**	

Figure 1. xStream Enterprise Architecture



State of Utah end users would access the hosted SAP environments via a MPLS connection (Provided by State of Utah). Additionally a VPN connection has been sized at 100Mbps however this can be decreased or increased depending on the exact requirements.

State of Utah end users accessing our enterprise platform would first hit the landing zone in a dedicated virtual local area network (VLAN) and dedicated virtual route forwarding (VRF). The next hop into the enterprise platform is a dedicated firewall (FW) context on a Cisco Firewall services module. After traversing the core, traffic hits another dedicated VRF and drops into the platform network and compute (CPU and Memory essentially a blade server) layer. All traffic is VLAN separated. At each compute host, a hypervisor based firewall and intrusion protection system (IPS) provides a dedicated client rule set to further ensure network security. All traffic transitioning from one zone to another are monitored by Intrusion Detection and Intrusion Prevention systems.

Traffic coming in via the internet hits the front-end perimeter with load balancing modules and multi-context Cisco firewalls. All traffic then passes through intrusion detection system and intrusion protection systems. As in the enterprise compute layer, every host in our demilitarized zone (DMZ) has a hypervisor-based firewall and IPS with dedicated client rule sets. Again, all traffic is VLAN separated as well.

Traffic that needs to traverse from DMZ to the enterprise runs through another dedicated FW context and IDS/IPS.

All of the State of Utah environments and data will be hosted in Virtustream's data centers within the continental United States.

Standard Services used in Virtustream's management environment and in all client environments including the following:

	• All Virtustream employees use Mandatory Strong 2 factor authentication (2FA OTP) Administrative Access to all systems. • Dedicated VLAN network segmentation and dedicated Virtual Route Forwarding (VRF) are used extensively to segregate environments and zones. • Perimeter Firewalls are used to segment internal and external environments as well as segregate security zones. Configuration, monitoring, auditing and logging are included. • Virtual Machine-based Firewall and Intrusion Prevention System (IDS) is installed on every virtual machine in the environment and is protected with Juniper's Security Gateway virtual firewall application and monitored service. Security Services that are standard components for Virtustream's management environment and are Optional Services for client environments including the following: • Managed Two-Factor Authentication ("2FA") is in use for all application systems. • Intel TxT Enabled Servers and Trusted Boot/Bios monitoring with Attestation Server and OS and VM support, including Geolocation and Geofencing according to NIST 7904 guidelines. • Secure operating system (OS) builds based on DoD Secure Technology Implementation Guide (STIG) guidelines are used to build Virtustream's Management and Administration Servers. • Server/File Integrity Monitoring (FIM) is installed in the PCI and VFC clouds. • Patching Regimen: Virtustream patches host servers, network devices, security devices, servers and related services in the Management Network on a specified routine (monthly or quarterly, depending on release schedules), or when there is a CERT or other authorized source of patch that requires immediate attention. Based on urgency and risk of the issue we will schedule the patch as appropriate and use change control. • Scanning regimen: vulnerability scanning is done on a monthly basis with additional 3rd party vulnerability scans done monthly. Additional scans are done when made aware of new vulnerabilities. Issues are classified and addressed according to Risk Classifications and are addressed with ITIL v3 change control processes. • Managed IDS signatures are routinely updated and the logs are monitored. • Anti-Virus is managed on all Management servers in Enterprise, PCI and, VFC clouds. • Logging Service of all servers, network devices, and security devices to a centralized log server system. • Governance Risk Compliance: We use a complete Enterprise Risk Management toolset to manage compliance reporting and continuous monitoring to all of our supported compliance frameworks. Virtustream's facility monitoring systems are complete as per specifications in NIST 800-53r3/4. We use site assessment methodologies and checklists as detailed in NIST 800-42. Our systems and facilities are monitored 24/7 for any exceptions or trends. Our tools, processes and CONUS (Continental USA) personnel monitor network, power, cooling, humidity, water leakage, fire suppression, power systems (utility power, UPS systems and generators) and site access. Virtustream's Physical Access Control Security is designed to protect the confidentiality, integrity, and availability ("CIA") of the cloud platform system and its data with the following security components: • Limited and controlled room access. • Logged and monitored access of all access control events. • Video surveillance and review of all access control events. • Biometric access control required to gain access to the Data Center. • US Data Center staff is limited only to US Citizens.

	• Locked racks and rooms with key log out/in process. • Data destruction policies and procedures. • Asset in/out policy and procedures. Physical access by authorized staff is controlled by badge systems and biometric access systems. All access of any kind is recorded and logged. Access lists are reviewed every 90 days. Employees that do not have a reason to have physical access are removed from our access management systems. Multiple high resolution and IR enhanced CCTV Cameras monitor our datacenters at all egress and ingress points as well as other sensitive areas. Security video footage is stored in a secure area for 90 days. Approved Visitor Access requires VISITOR Badges and bright lanyards that are specifically different from employee badges. Visitors are required to produce and surrender a state or government issued photo ID during the visit, have a pre-approved reason for the visit, and have the escort witness the sign in and out procedure. Visitors are escorted continuously through approved areas of the facility. Visitors are not allowed access to following areas of the data center under any circumstances: • Cloud hosting areas. • Networking and telecommunication areas. • Guard areas. • Power vaults.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

FireEye	Background verification for employment candidates is a mandatory component of FireEye's hiring process. All personnel are required to sign a confidentiality and non-disclosure agreement agreeing not to disclose proprietary or confidential information including client information to unauthorized parties. Security awareness training program is in place to maintain the skill level of personnel regarding security and privacy expectations and best practices. All FireEye personnel at all levels are trained and notified of information security and privacy requirements and personnel responsibilities.
VirtueStream	Virtustream employees who are assigned to IaaS must pass a Virtustream background investigation. In addition, Virtustream employees assigned to the IaaS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone which includes access to sensitive data.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

CA	At CA Technologies, we comply with a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. We ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks and adhere to the highest industry compliance and security policies. CA offers a variety of SaaS solutions, details for each offering has been provided in Exhibit 1 and 2 of this proposal.
Google	All connections from customer end point devices to Google's Front End Servers are encrypted with enforced HTTPS sessions using Forward Secrecy. Google websites and properties use robust public key technologies: 2048-bit RSA or P-256 ECDSA SSL certificates issued by a trusted authority (currently the Google Internet Authority G2).

	All data in transit between Google's Data Centers traverses across Google's private fiber network using a customized, proprietary encryption technology. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. These methods of encryption are fully managed by Google and Google's Key Management Servers based on 128-bit or stronger Advanced Encryption Standard (AES). Encryption Keys and Ciphers Supported by Google Protocols TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.04 QUIC Cipher suites ECDHE_RSA with AES ECDHE_RSA with 3DES ECDHE_ECDSA RSA with AES RSA with 3DES Signing keys RSA 2048 ECDSA P-256 Hash functions SHA384 SHA256 SHA1 MD5
Salesforce	Government Cloud Encryption Capabilities: As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2 cryptographic implementations for data being transferred between the State's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below. Data In Motion: Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048- bit Public Key. Our service uses International/Global Step Up certificates. We support one- way TLS, in which customers create secure connections before sharing private data. Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Data At Rest: NIST SP 800-53 Rev. 4 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different

	mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data. For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with AES encryption, for a selection of custom fields included in the Force.com Platform and Salesforce Services. Field-level encryption ensures the data associated with designated fields is encrypted in storage.	
SAP	Ariba	Sensitive data elements, including PCI Primary Account Numbers and system account parameters for internal application communications, are stored in Ariba databases encrypted by the AES (Advanced Encryption Standard) and Triple DES (Data Encryption Standard) encryption algorithms with a minimum key length of 128 bits. Encryption technology is also applied for the client connection to the Web site and to the hosted application passwords in storage. Customer user passwords are one way hashed using SHA256 and salted with random data. Limited Ariba Operations personnel have data query access and monitoring rights for the Ariba Hosting program.
	Fieldglass	
	Hanna	SAP provides for enterprise-grade and industry-standard security. SAP HANA Enterprise Cloud datacenters are enterprise-class security with enterprise-class protection including data encryption, network encryption, firewalling, network isolation, and intrusion detection. HANA data is protected in multiple different ways. SAP HANA Enterprise Cloud is a managed cloud service that employs either a VPN or MPLS connection for transit. By default VPN is encrypted and MPLS can be encrypted. The customer procures the method of connection. At installation, HANA data can be encrypted using a feature called Data Volume Encryption. This encryption protects data in the persistence layer. Storage volume access is restricted to the customer account that created the volume, thus denying all other customer accounts the permission to view or access the volume that includes data isolation, masking, zoning and Logical Unit (LUN) binding. Strict user and access management, authorization management according to the need-to-know principle for administrative accounts, and security logging and security monitoring for critical activities or access, also protect data stored in HANA.
	Hybris	The Hybris platform uses SSL (https) for both the web application tier (browsers and WebService APIs) as well as communicating with back office systems. Data at rest is something that has to be taken into consideration in the application requirements by the partner/customer or PS teams. If encryption is required the application teams need to work on implementing the methods to encrypt and secure the data, for example encrypting data fields in the database.
	SuccessFactors	Each customer's data is maintained in a separate database schema eliminating data segmentation breaches. Each schema has separate authentication credentials and assigned resource profile to restrict access rights and resource consumption. Encryption for data at rest uses the AES256 cipher. All application access is encrypted-in-transit over HTTPS with 128-bit TLS encryption.

FireEye	At rest: Data are collected using automated batch and real-time processes and by manual personnel-driven actions via an Analyst facing Portal. Any information that is collected may be stored temporarily within appliances attached to our customers' networks and may subsequently be transmitted back to one or more FireEye datacenters. Data transmitted from a customer's network to a datacenter travels over a strong encryption Virtual Private Network ("VPN") established by the appliances. At transit: FireEye's network sensors are configured to collect full packet capture of customer network streams, including those originating from or destined to potentially malicious IP addresses, matching signature-based network indicators of compromise, results of domain name lookups, and full e-mail messages including headers, content and attachments. This information is primarily stored on-site on the appliances and only meta data matching FireEye / Mandiant indicators of compromise are sent to FaaS.
VirtueStream	Virtustream's use of Intel® Trusted Execution Technology (Intel® TXT), a hardware-root of trust security feature, and Intel® AES-NI encryption acceleration helps secure and protect virtualized environments against malware and provides more of the critical infrastructure and data protection assurances needed to enable trusted multi-tenancy in the cloud. Virtustream offers solution for data-at-rest and data-in-transit encryption solution for our customers as optional service, as most of our customer environment is only accessible via private network and only to the internal users of the customer. Solutions available to our customer as follows. 1. IPSEC VPN Tunnel for data-in-transit and 2. VM level encryption for files and databases 3. Encrypted Backup (all backups are encrypted by default) The technologies of encryption available throughout the entire data lifecycle and all are FIPS 140-2 compliant. a) DB and File System Encryption b) Encrypts file system and volume data transparently to: i) Applications ii) Databases iii) Storage Infrastructure c) Integrated Key Management d) High Efficiency Encryption i) Centralized Key Management ii) Policy Management iii) Detailed Auditing iv) Highly Available v) FIPS 140-2 Certified Hardware Appliance vi) Very Low Encryption Penalty due to Intel AES-NI enabled chip sets used e) Encryption of Virtual Machine, OS and App i) Integration of SafeNET Protect-V ii) Logging of all image access f) Encryption in Archive g) Implements Encryption, Access Control, Auditing on Host (LUW) h) Kernel Level Driver – Win i) File System – Unix/Linux j) Support for file systems and raw partitions k) Highly efficient block encryption

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

CA	CA Technologies abides to contractual requirements for notification, in addition to working with legal to ensure compliance with regulatory requirements. There may be cases where incident analysis completion is a requirement for confirming the breach, and / or its impact and data leakage boundary. Prior to completion of this activity, CA may not have the needed conclusions for customer communication. Once subscriber data has been identified as part of the investigation, said subscribers will be notified as soon as possible and not longer than 5 days. A report of the incident will be available and distributed to clients within 30 days. Please note that none of the offerings proposed as considered payment products and are not intended for use of storage of cardholder data.	
Google	Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing. If Google becomes aware of a Data Incident, Google will promptly notify Customer as permitted by law of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by the Purchasing Entity in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting).	
Salesforce	Salesforce will promptly notify the State (within 48 hours, reflected in a negotiated agreement between the parties) in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to the State's administrator and Security Contact (if contact is submitted by State and contact information is kept up to date), and public posting on trust.salesforce.com.	
SAP	Ariba	Ariba has developed a computer security incident response team. Following policies and procedures, this team responds to suspected security incidents to mitigate risks and damage. The team conducts response and forensic analysis of systems and network traffic. This information can be used to assist with prosecution if a security breach is detected and the offender caught.
	Fieldglass	SAP Fieldglass' security team is responsible for managing security incidents and all communication is conducted via the respective account managers to ensure timeliness. The process is defined within the Incident Response Management Standard. Customers are notified of an incident within 48 hours.
	Hanna	SAP will notify via defined communication channels within 36 hours of a confirmed data security breaches to the affected customers. The report will detail the following information: • Details relating to the security incident that has occurred, known at the time of notification. • IT infrastructure and/or application affected by the security incident. • Overview of the performed mitigation actions to restore the security, documented within the incident report form. • All further applicable requirements by country regulations "on obligation to notify" will be met.
	Hybris	Since we do not allow for CC data to be transmitted, stored or processed in our environment, we regularly scan the customer environment in case this is done without our consent. However, we do have a CSIRP in place, in which we would notify the customer and our internal Forensics team in the event that a customer environment should be breached.
	SuccessFactors	Upon the occurrence of a data breach, initial communication is distributed to the appropriate individuals and an escalation process is followed. Upon

		becoming aware of the incident, measures are promptly taken by the team to resolve the situation. All affected customers should be informed within at most 36 hours of confirming a potential breach in the privacy of their data. Following incident resolution, follow-up is required to ensure that the incident has been resolved effectively and that the threat is no longer present. We are aligned with ISO 27k standards for event and incident management and have formal incident management policies and processes in place. These policies and procedures are tested in the ISO 27k and SOC 2 audits.
FireEye	FireEye has a documented policy for incident management that has been approved by management and communicated to appropriate constituents and owners. It is continuously maintain and reviewed annually. The plan has a reporting structure and escalation path. An incident response team with defined roles and response related qualifications are available 24x7x365. The team maintains chain of custody for evidence during the incident investigation. There is a process for reporting client notification for regulatory, legal and contractual issues after a breach if a breach were to be confirmed. If a confirmed breach were to occur a management team would review all the factors and develop a remediation plan to mitigate.	
VirtueStream	There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'. The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement. The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS. The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan. As the incident progresses and has more impact (i.e. severity level increases), the escalation process will be used to engage appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.	

8.7 Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

The end of life activities for each Purchasing Entity will vary based on the type of service they are currently using and the service that they will be moving too. All Purchasing Entities will be notified in advance of any end of life service so that the Purchasing Entity can work with Carahsoft and the service providers to develop a plan exporting and transitioning data.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

At all times during the course of the Service, the Purchasing Entities will have access and ownership of their data. The Purchasing Entity is free to download or access the data through a variety of means based on the service at any time during their service period.

8.8 Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

CA	APM	If unable to resolve in a timely manner, all customers will be notified via email to the registered admin
	MAA	Customers are kept abreast with progress during incidents, including outages. CA utilizes best-of-breed notification system which enables customer contacts to self-subscribe to different types of notifications that they would be interested in. A DR plan has been created should the extended down time result in DR declaration.
	CA Agile	We would failover to our warm data center in order to restore access to the application as quickly as possible. This is done according to our Disaster Recovery Plan
	ASM	If unable to resolve in a timely manner, all customers will be notified via email to the registered admin. Failover from the primary to DR site may be utilized if the extended amount of time warrants declaration of DR.
Google	Due the redundant nature of the Google infrastruture there is no expectation of any extended downtime. If a data center in use by any of your end users suffers a catatrophic failure, Google's dynamic health monitoring would just reroute the session to a different data center.	
AODocs	All the AODocs data is hosted on the Google Cloud Platform infrastructure. AODocs does not manage any physical infrastructure. Due the redundant nature of the Google infrastruture there is no expectation of any extended downtime. If a data center in use by any of your end users suffers a catatrophic failure, Google's dynamic health monitoring would just reroute the session to a different data center.	
Virtru	Notify users that Virtru service is unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best	

	redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds, all with an average up time of 99.9+ percent.
ServiceNow	ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region. ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways: •In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center. •Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability. This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized. RTO is 2 hours. RPO is 1 hour. See the "ServiceNow Security, Operations, and Compliance White Paper" included with this response for more information.
QTS	In the rare instance of failure of the commercially-delivered electrical power, back-up systems at each QTS data center start instantaneously. Batteries provide power for the first 12-15 seconds while on-site diesel generators spin up to synchronize their output with the battery-supplied feed. Once on-line, the generators can supply power indefinitely, and the IT equipment on the data floor as well as critical infrastructure components are all unaffected. While the basics of reliable power seem simple, none of this is taken for granted. Battery banks are sized to provide 15 minutes of power, well beyond the 15 seconds that it typically takes generators to come on line. Inspections are conducted daily and quarterly to ensure that the battery banks are prepared at all times. The diesel generators are inspected by running them each month to circulate and condition the fuel, then running them annually under the full simulated load of the current IT equipment on the data center floor. Factory technicians inspect and maintain the generators semi-annually. Quantities of fuel sufficient to support 48-72 hours of

	operation without resupply are stored on-site, and re-supply contracts are in place with multiple providers to have fuel delivered as soon as the generators come on line.	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes. Disaster recovery options are included for all Ariba Cloud Services. In the event of a fail-over to the disaster recovery site, no customer changes are required as all URLs that customers use to reach the applications will continue to work. Ariba will notify customers via their email addresses in the event of unplanned downtime. Internally, Ariba uses a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster: Local Ariba staff maintains the hardware remotely. Ariba maintains the application software. Processes are in place to keep database and fileservers in sync between primary and backup data centers. The failover process of all parts of the infrastructure is automated. In the event of a catastrophe, Ariba will declare the primary data center "down" and locally the script will be run to switchover and start the applications at the remote data center. Ariba tests power outage backup scenarios and the Disaster Recovery Plan on a periodic basis to ensure it is up-to-date, successful, and effective.
	Fieldglass	Customers are notified of unscheduled downtime immediately via email. Updates are frequently emailed out until the issue has been resolved. Customers are notified of scheduled downtime 5 days prior via email.
	Hanna	In case of a disaster depending on the infra & technical architecture defined during HEC technical assessment workshop, systems could fail over to HA node. If DR (optional offering) is selected, the systems could move to secondary DC that where contracted with a DR option & HEC declaring DR. Regular system downtime for patching etc. is planned in advance with the customer and typically follows customers maintenance schedules.
	Hybris	SAP Hybris offers continuous 24/7 systems monitoring in-place, which automatically notifies you, SAP Hybris support and optionally your designated implementation partner in the event of any monitored system problem. Tools used for monitoring include HP Sitescope and Nagios. This service ensures quick response times to emergency problems. Standard monitors are in place for basic site availability. Customer can utilize additional 3rd party monitoring services should it wish to add additional monitoring. Upon request, monthly or quarterly reviews are offered to review performance over the period. When a system problem occurs, in addition to monitor alerts sent to the customer, SAP Hybris support may send emails to a designated customer notification email address to provide status, updates or further detailed information. In addition, a support ticket would be created which would include such information.
	SuccessFactors	Our infrastructure architecture is designed with high availability in mind, and engineered for resiliency. All major components are redundant, including power, HVAC, fire suppression, and the physical components of our network. Production data centers have strict access controls, and are continuously

		staffed and monitored to help prevent acts of sabotage or vandalism. All production data centers are ANSI/EIA/TIA-942Tier III/IV facilities, and are ISO 27001 certified. Production data centers are also geographically dispersed to help prevent a single event from affecting more than one data center. In the event a production data center has an outage we failover to an alternate data center in the same geographic region to minimize impact to customers. Our Cloud Operations teams are also geographically dispersed, working in offices in the US, Europe, South America, and India. Should an office be impacted by an environmental event or pandemic, other offices can continue operations. Aspects of the plan are described in the SOC reports, Disaster Recovery Plan ("DRP") and Business Continuity Plan ("BCP") solutions are dependent on several factors. The customer may be responsible for parts of the recovery/continuity activities.
VMware	VMware vCloud Air leverages proven VMware High Availability technology to minimize the risk of extended downtime. In the unlikely event that an extended outage does occur, VMware will support guide the customer's efforts to restore services to an alternative vCloud Air or vCGS datacenter. We will also provide remedies in the form of service credits as outlined in the following VMware vCloud Air, vCGS, Vmware AirWatch and VMware Identity Manager SLAs.	
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.	
VirtueStream	In the event of extended downtime affecting production systems, Virtustream and customer would jointly evaluate the situation and mutually decide on failover declaration, whereby Virtustream would then execute the failover plan to restore customer operations to the secondary data center.	

b. Suffers an unrecoverable loss of data.

CA	APM	Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs.
	MAA	MAA data is backed up fully daily. The maximum data loss would be the previous 24hrs.
	CA Agile	We have implemented a physical standby database in both hot/Live site as well as warm/standby sites using Oracle Data Guard with real-time apply to achieve the stated recovery objectives.
	ASM	Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs.
Google	Google performs real time data replication to avoid unrecoverable data loss. Customers that configure the retention policies in Google Apps Vault can ensure that end users can not inadvertently or maliciously delete email in advance of any defined retention schedules.	
AODocs	AODocs data are stored in Google AppEngine and Google Drive: - The data stored in Google AppEngine are backed up every day. The application is hosted on Google Cloud Platform infrastructure and benefits from the network security described in this whitepaper: https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf - Data stored in Google Drive is managed by Google within its multiple servers location. Altirnao does not manage this infrastructure. Google Drive can be backed up by third party tool such as Backupify.	

Virtru	Notify users that data within Virtru is unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	To maximize availability, the service is delivered using multiple world-class data centers supporting primary and replicated disaster recovery instance, plus a separate production-class lab. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance. The Salesforce services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS cloud developed a OPS_POL_54_QTS-FC_Contingency_Planning_Policy (v1.2 – 2/6/14), detailing the policies, procedures, roles and responsibilities of key personnel in the event of an emergency and/or disaster.	
SAP	Ariba	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
	Fieldglass	The maximum data loss timeframe is guaranteed to be less than three hours; however, offsite backups are performed every 15 minutes so the timeframe is actually much shorter.
	Hanna	Data loss is defined by RPO & RTO. HEC has a maximum RPO of 30 mins & RTO of 12 hours.
	Hybris	For a cloud solution, data backup and restore is handled by SAP. SAP shall follow its archiving procedures for Customer Data as set out in the SAP Hybris Commerce, cloud edition Services Description. In the event of any loss or damage to Customer Data, SAP shall use commercially reasonable efforts to restore the lost or damaged Customer Data from the latest back- up of such Customer Data maintained by SAP in accordance with the archiving procedure described in its SAP Hybris Commerce, cloud edition Services Description. SAP shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party, (except those third parties sub- contracted by SAP to perform services related to Customer Data maintenance and back-up).
	SuccessFactors	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
VMware	VMWare IaaS Services As discussed in detail in section 8.8.2.1.a below, VMware IaaS services are architected to minimize the risk of unrecoverable data loss. In addition option services such as vCloud Air Data Protection can be leveraged to further mitigate any risk. VMware's vCloud Air policy regarding data loss can be found in the vCloud Air Terms of use. VMware's vCloud Government Service policy regarding data loss can be found in the vCloud Government Service Terms of Service AirWatch Hosted Services AirWatch Business Continuity and Disaster Recovery strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises. AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure timely server recovery. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.	

	• Due to FOIA restrictions and the competitive nature of the EMM marketplace, we cannot provide specific details regarding recovery strategies or timelines.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Multiple copies of customer data exist in multiple datacenters – in the primary datacenter, there is the production copy and a local backup. The local backup is replicated to a secondary datacenter and the production datastores associated with coreVM's are also replicated at regular intervals to the secondary datacenter. If NASPO feels that additional steps/redundancy are required to maintain recoverability, Virtustream is open to discussion.

c. Offeror experiences a system failure.

CA	APM	Disaster to the CA Technologies corporate network in New York will not affect customers' service. Secondary services, such as domain name services will be routed through the secondary CA Technologies network in Illinois. CA has a BCP plan in place to direct its services. The SaaS environment is separate from the CA corporate network and a service specific disaster recovery plan is in place.
	MAA	Customers would be notified in advance, and given ample time to retrieve their data.
	CA Agile	We enable all of our employees with the ability to be able to work remotely and provide remote network access to ensure business functions can continue. All corporate infrastructure has redundate systems that can be utilized in the event of failure.
	ASM	Customers would be notified in advance, and given ample time to retrieve their data manually or via the ASM API.
Google	Google's corporate network is separate from it's production infrastructure. Google is a global organization that has support personnel located at key office installations and tests our business continuity programs annually. These tests are to validate that if corporate headquarters is off the grid that criticial business functions can be picked up by other staff.	
AODocs	AODocs runs 100% over Google's Cloud Platform infrastructure that is naturally redundant, and all AODocs internal systems such as technical support, email, collaboration, source code hosting, etc are run on cloud based services. AODocs personnel can work from any physical location without any business disruption and they do work from remote locations on a regular basis. If one of the AODocs facilities were to be temporarily unavailable due to a natural disaster, AODocs personnel would be able to perform their work without significant interruption.	
Virtru	Notify users that Virtru is or will be permanently unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	Please see response to items a. and b. above and d. and e. below. Salesforce has documented Disaster Recovery and Business Continuity plans for critical business functions. The Disaster Recovery and Business Continuity plans are tested at least annually. A post mortem documenting the results of the disaster recovery tests can be provided to customers with a signed NDA in place. Business continuity plans are updated each year, including the list of business processes, recovery time objectives, and key resources. Senior management is included in this process. Business continuity plans are exercised on an annual basis. Action items and lessons learned are tracked from each incident and exercise conducted. Action items are prioritized and tracked until	

	closed. Salesforce has developed additional procedures, processes and plans, including a Pandemic plan. Salesforce also recommends customers also devise their own backup strategy for their data, as there is a fee for customers to request for restoration from Salesforce backups. Salesforce provides multiple ways for our customers to obtain periodic backups of its data. We offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Salesforce also supports data replication, which allows customers to store and maintain a local, separate copy of their organization's Salesforce data including the META data (logins, etc.) for specialized uses, such as data warehousing, data mining, custom reporting, analytics, and integration with other applications. Data replication provides customers with local control and the ability to run large or ad hoc analytical queries across the entire data set.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS has established an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable. The QTS cloud hosting facilities in Richmond, VA (RIC1) and Atlanta, GA (ATL1) have agreements with each other to restore services in the event that one of the sites becomes unavailable. Both facilities are QTS managed facilities and are always available to meet the recovery time and recovery point objectives for the system. Agreements are in place to allow QTS to access resources at the alternate processing site physically and via the QTS client network. Richmond and Atlanta Datacenters are independently operated datacenters that offers disaster recovery services to customers. The contingency approach ensures that hardware and software components needed for recovery efforts are already at the alternate facility. QTS ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Network circuits, networking infrastructure, storage, virtual servers, and management components required to resume operations are available and configured at the alternate site.	
SAP	Ariba	"Ariba modules automatically persist object state to the underlying relational database as users work. When a user performs a significant action, for example, adding an item to an order, performing an approval, etc., the Ariba application tier is aware of the change and automatically saves the relevant object state to the database. This provides transparent persistence of the user's work without the user having to “save” or “submit” changes to avoid losing work in the event of failure or session timeout. This in turn means that the loss of any connections between the tiers or failure of one of the tiers will not leave data in an inconsistent state. While object data is cached in the middle tier for performance, the official record is stored in the database to avoid any potential data loss or corruption. This means that recovery for Ariba modules is implicit and automatic. When the modules start, they retrieve the state of the various business objects from the underlying database as needed for user sessions. If an Ariba module fails, there is no special application recovery process other than restarting the module. The Ariba module will automatically connect to the database and as clients login and commence working, all required business object data will be retrieved from the database."

	Fieldglass	Fieldglass' business continuity program (BC Program) was established to ensure that, after a complete disruption of its Chicago and/or Naperville, Illinois offices, all employees and the functions for which they are responsible, are capable of continued operations in less than one business day. This includes office space as well as all equipment and supplies needed to continue its operations without an interruption in customer services. Fieldglass' BC Program is integrated into all facets of the company due to the criticality of the product that it sells and supports. As such, representatives from all areas of the company are responsible for ensuring that they are familiar with their duties and responsibilities during a disruption and how to recover their areas after the disruption occurs.
	Hanna	Service Level Credits Where SAP fails to meet a Service Level, SAP will be liable to Customer for the corresponding Service Level Credit as set out in this section. The Service Level Credit is calculated as the sum of the Service Level Credits for both DEV/QAS and PRD for the TA Service Level defined in section 5.1 above. SAP will deduct the amount of any Service Level Credits owed to Customer from the next invoice (or, if there is no such invoice, by bank transfer to such bank account as Customer may specify in writing). Customer agrees that under no circumstances will the total maximum Service Level Credits: (i) for any one month, exceed 100% of the Service Fee for that month; and, (ii) for any given contract year, exceed in the aggregate an amount equal to one- third of the annual Service Fee charged for the contract year (or one third of the total Service Fee charged if the Term as defined in the applicable Order Form is less than one (1) year). Customer acknowledges that the Service Level Credits defined hereunder are the sole remedy for SAP's failure to meet the specified Service Level. 5.6 Termination for Service Level Failure Customer may terminate the applicable Order Form with thirty (30) day's termination notice in writing to SAP, if SAP misses a Service Level as specified in this Supplement for three (3) months in sequence. Customer may exercise this termination right only within thirty (30) days after receipt of the respective Service Level report that documents the applicable Service Level failure that would cause such termination right to accrue in Customer.
	Hybris	SAP isn't likely to go out of business in the near future. However, our contract states the following: Upon expiration or termination of the Agreement, SAP may destroy or otherwise dispose of any of Customer Data in its possession unless SAP (i) is requested by Customer to extend the term of the Order Form as permitted in the Order Form to allow Customer to retrieve Customer Data, or (ii) receives, no later than thirty (30) days after the effective date of the termination of this Agreement, a written request for the delivery to Customer of the then most recent back-up of the Customer Data. SAP shall use reasonable commercial efforts to deliver the back-up to Customer within thirty (30) days of its receipt of such a written request, provided that Customer has, at that time, paid all fees and charges outstanding and owed at termination. Customer shall pay all reasonable fees and expenses incurred by SAP in returning or disposing of the Customer Data.

VMware	AirWatch Hosted Services AirWatch Business Continuity (BC) strategies include clear policies and procedures as well as robust, regular testing exercises. Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff. • Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers. • Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources. • Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate the risks of a system failure. Additional levels of protection include regular system backups (stored locally and replicated offsite) as well as automatic storage replication to a secondary data center to facilitate the ability to restore operations in the event of a system failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

CA	APM	CA provides an SLA of 99.8% uptime, which can result in unforeseen outages of ~1.5 hours per month. In the event of a failure to meet a SLA threshold , Customer is entitled to a number of days of credit.
	MAA	Using DB clustering technologies, multiple copies of data are maintained helping in recovery of the data.
	CA Agile	We can meet this requirement.
	ASM	Data is replicated from the primary (production) to secondary (DR) continuously. In the event of catastrophic loss of live data a failover to the DR site would be necessary.
Google	Google's RTO is zero.	
Virtru	See 'Virtru Incident & Breach Policy'	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at primary data center facility without stopping access to the application. For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency.	
ServiceNow	Please see our response for 8.8.1a	
QTS	As defined in QTS OPS_POL_54_QTS-FC_Contingency_Planning_Policy (v1.2 – 2/6/14), QTS cloud has identified the following potential accessibility problems: • Network Outage – Short Term • Network Outage – Long Term • Facility Power or Environmental Outage – Short Term	

	• Facility Power or Environmental Outage – Long Term • Serious Facility Damage – Short Term • Serious Facility Damage – Long Term or Permanent Both the RIC2 and ATL1 QTS cloud Infrastructure is an Active/Active system and can operate independently of each other indefinitely. If QTS cloud determines that any single event (network, power, facility damage) presents a long-term threat, QTS immediately conducts an emergency meeting and plan to remedy or relocate infrastructure to a viable facility."	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes.
	Fieldglass	Fieldglass offers the following: • RTO = No more than 48 hours • RPO = No more than 6 hours. Warm site replica with 100% processing power of original site. Disaster recovery site can run without need from resumption.
	Hanna	See our RTO and RPO info below
	Hybris	For a cloud solution, data backup and restore is handled by SAP.SAP shall follow its archiving procedures for Customer Data as set out in the SAP Hybris Commerce, cloud edition Services Description. In the event of any loss or damage to Customer Data, SAP shall use commercially reasonable efforts to restore the lost or damaged Customer Data from the latest back- up of such Customer Data maintained by SAP in accordance with the archiving procedure described in its SAP Hybris Commerce, cloud edition Services Description. SAP shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party, (except those third parties sub- contracted by SAP to perform services related to Customer Data maintenance and back-up). Both IDS and IPS are included the SAP Hybris Commerce, Cloud Edition The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer. Upon expiration or termination of the Agreement, SAP may destroy or otherwise dispose of any of Customer Data in its possession unless SAP (i) is requested by Customer to extend the term of the Order Form as permitted in

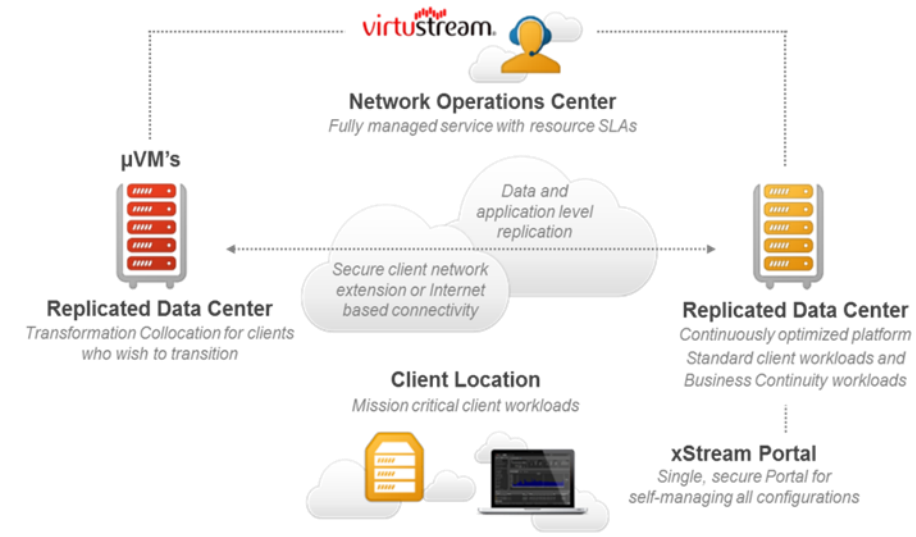
		the Order Form to allow Customer to retrieve Customer Data, or (ii) receives, no later than thirty (30) days after the effective date of the termination of this Agreement, a written request for the delivery to Customer of the then most recent back-up of the Customer Data. SAP shall use reasonable commercial efforts to deliver the back-up to Customer within thirty (30) days of its receipt of such a written request, provided that Customer has, at that time, paid all fees and charges outstanding and owed at termination. Customer shall pay all reasonable fees and expenses incurred by SAP in returning or disposing of the Customer Data.
	SuccessFactors	RPO and RTO are defined in the general terms and conditions
VMware	VMware Response: VMware IaaS Services VMware DR service. We can discuss specific recovery information under NDA to participating entities during task order negotiations as required. AirWatch Hosted Services We can discuss specific recovery information under NDA to participating entities during task order negotiations as required.	
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.	
VirtueStream	Basic Plus microVM's are designed for mission-critical workloads and for systems that require DR, addition of reserved compute capacity in a secondary datacenter (i.e. Reserve uVM) and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center. RPO and RTO for core microVM's are 15 minutes and 2 hours respectively.	

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

CA	APM	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 72 hours
	MAA	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 72 hours
	CA Agile	RTO: 2 hours RPO: 12 hours
	ASM	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 24 hours
Google	RPO/RTO objectives are zero hours.	
AODocs	AODocs is hosted on Google App Engine which is designed to be highly available. Our standard SLA is 99.5% . Specific financial penalties can be discussed as part of the AODocs license contract. Google App Engine is running in multiple datacenters on multiple continents.	

	AODocs data is backed up on a daily basis, and backups are stored on the highly redundant Google Cloud Storage. Backups are retained for at least 90 days	
Virtru	See 'Virtru Incident & Breach Policy'	
Salesforce	For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS DRaaS will support all of your mission-critical application needs and enables you to achieve a RTO within minutes and RPO of just seconds.	
SAP	Ariba	See above
	Fieldglass	Fieldglass offers the following: • RTO = No more than 48 hours • RPO = No more than 6 hours. Warm site replica with 100% processing power of original site. Disaster recovery site can run without need from resumption.
	Hanna	For disaster Recovery, SAP HEC offers the following RTO & RPO 1. HANA Database RTO - 12 hours, RPO - 30 minutes 2. Sybase ASE Database RTO - 12 hours, RPO - 30 minutes
	Hybris	In the case of catastrophic failure to your primary production data center, we offer anywhere from best efforts to enhanced DR solutions. Enhanced DR options translates to either RTO of 8 hours and RPO of 1 hour for a warm standby solution, or RTO of 30 minutes to RPO of 30 minutes for a hot-site. Customers have 3 choices in DR sites: • as part of our base offering, best effort DR, we would bring your site back up in an alternate datacenter which is a minimum of 500 miles away from the primary datacenter. We would actually push your project server images to the alternate datacenter, but we would still need to set up your various interfaces, 3rd party services, etc, which could day a few days. • 2nd would be to have your DR site managed by hybris Managed Services. • 3rd would be to use your own DC as a DR site, We would need to set up a technical call with our combined teams to synch up on the replication strategies. • Our DR services utilizes VMware Site Recovery Manager with storage-based replication. • For enhanced DR, we would include one annual DR test, but more can be added if required. It also includes a customer specific DR and Business Continuity plan.
	SuccessFactors	Within the contract/subscription agreement, there are provisions for data recovery in the event of disaster. SLA's for RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are defined in the contract. We will prioritize data recovery based upon our contractual obligations for each customer, concerning RTO and RPO.

VMware	VMware IaaS Services Provide the RPO and RTO for DR, point to SLAs for others. RTO – 4 hours or less RPO – 15 minutes to 24 hours – time is configurable by user but there is a bandwidth consideration for shorter replication times. VMWare AirWatch AirWatch Business Continuity (BC) and Disaster Recovery (DR) strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises. • Business Continuity – Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff. o Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers. o Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources. o Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff. • High Availability and Disaster Recovery – AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss. Due to FOIA restrictions and the competitive nature of the EMM marketplace, we cannot provide specific details regarding recovery strategies or timelines.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Virtustream's solution will have a Recovery Point Objective (RPO) of 2 Hours and Recovery Time Objective (RTO) of 30 Minutes for all disaster recovery enabled workloads. The Virtustream Cloud has been designed to deliver continuous operations. The platform is architected to be highly available, with SLAs as up to 99.99%. All infrastructure systems are run in at least an N+1 model and have been designed with no single points of failure. All of the data center facilities and infrastructure has redundant power supplies connected to separate circuits from separate power feeds. Every device is connected via redundant pathways at a LAN/SAN/WAN layer. State of Utah can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01. The State of Utah solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, State of Utah's production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target RPO is 30 minutes for virtual machines with a 2 hour RTO. All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers.

	Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process. **Figure 2. Integrated Disaster Recovery** Virtustream's cloud platform includes integrated disaster recovery (30 Min RPO & 2 Hr RTO) and backup. 

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

CA	APM	Backups are stored on disk only
	MAA	Backups are stored on disk only, sync'd between data centers for DR purposes.
	CA Agile	Full database backups are taken once per week, both to onsite and offsite (our warm data center, not a separate 3rd party) systems. Incremental backups are run nightly. Backups are retained for 21 days after which time they are simply aged out and over-written. In addition, snapshots of database transactions are taken every hour to an disaster recovery site allowing for emergency disaster recovery with maximum of 1.5 hours of data loss due to catastrophic onsite failure (fire in cage, natural disaster, etc. at data center). Backups are tested monthly and a full disaster recovery process to the offsite application cluster is tested semi-annually.
	ASM	Backups are stored on disk only, sync'd between data centers for DR purposes.
Google	Keeping in mind that Google stores customer data in encrypted chunks or shards on several servers at several data centers backups should not be considered customer specific. Daily backups of each server are performed to encrypted tapes at each data center.	
Virtru	We perform live database replication to a separate redundant database in Oregon and offline as well in a separate Amazon AWS Region	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.	

	Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process. The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.	
ServiceNow	While Advanced High Availability as described in 8.8.1 is the primary means to recover data and restore service in the case of a service disruption, in certain cases it is desirable to use ServiceNow's more traditional data backup and recovery mechanism. This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism. ServiceNow stores production instances in two geographically separate regional data centers, with sub-production instances hosted in a single data center. Backups of the two production databases and the single sub-production database are taken everyday for all instances throughout the private cloud infrastructure. The backup cycle consists of four weekly full backups and the past 6 days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database then it will also be encrypted in the backups. Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.	
QTS	QTS operates and manages high-performance, multi-tenant platforms on which customer system and data file backups can be created and retained for rapid restore of files/volumes. Data can be stored on tape or disk, depending on QTS location, and can reside locally in a QTS data center or off-site. If there is a need for off-site data retention, the backup medium is tape. QTS can also replicate the backed up data from the primary site to a secondary (remote) site to address geographically remote storage and DR requirements. Secure: QTS utilizes a separate, secure gigabit backup network with private VLAN security. Physical security is monitored using a priority badge access system to limit access to the tape libraries, disk arrays, servers, and network infrastructure. From the application, the backup software controls access to the data stored on tape, and access security is limited to QTS staff only. Scalable: QTS backup systems are highly scalable, and capacity can be quickly added as needed.	
SAP	Ariba	Our primary data center is Equinix, in San Jose; CA. Ariba's backup data center is CenturyLink in Sterling, VA. We make many copies of our data to insure no data loss happens: Data is stored in databases on high-availability storage disk-based system in primary datacenter Data is copied as backup to high-availability disk storage in the primary datacenter Data is copied to tape and kept in the primary data center Data is copied to tape and kept in an off-site tape storage facility (Iron Mountain) in Union City Data is replicated to databases high-availability storage disk-based system in the backup datacenter Data is copied as backup to high-availability disk storage in the backup datacenter Data is copied to tape and kept in the backup datacenter

		Data replication to the remote datacenter happens in near-real time. Data is backed up to the backup disks multiple times a day (in each location) Data is written to tape once a day (in each location) These processes and procedures are audited against the ISAE 3402 standard. Our auditor verifies we can restore from these backup methods.
	Fieldglass	All data in the Fieldglass system is stored within our clustered databases. Full backups daily, 15 minute incremental backups, and replication from center to center of backup data continuously.
	Hanna	The backup of SAP systems in HEC is executed on EMC DataDomain deduplication storage. This is done using EMC Networker for backup and administration. The backups on Site A are also replicated to remote Site B.
	SuccessFactors	Data backup is undertaken as follows: storage system snapshots every 24 hours, nightly incremental database backups, and weekly full database backups. These are all standard and provided as part of our hosted service. All backups are stored on disk in the primary and backup data center facilities for 30 days. Database backups are encrypted and stored at a customer's "primary" location, as well as the "alternate" warm-site location for redundancy and disaster recovery purposes. If the customer's primary location is defined as the data center in Amsterdam, NL, then copies of their database would be encrypted and streamed in a secure manner to the data center based in St Leon-Rot, DE, and vice versa. The backup is stored on Storage Area Network systems encrypted with AES-256 bit by encryption appliance. Backups are retained for 30 days. Our Log File Retention Policy is designed to meet or exceed the most stringent industry standards. Archiving of data is the customer's responsibility.
VMware	VMware will provide the following services to participating entities with respect to Data Recovery: •Data protection, such as routine backups, for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. •Data and infrastructure restoration for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. Participating entities will be responsible for the following services with respect to Data Recovery: •Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air virtual machine's or storage devices, configuration settings, etc. •Data, content, virtual machine and configuration restorations for assets accessed or stored on your vCloud Air account. Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important virtual machine data and content hosted in your vCloud Air IaaS environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their virtual machine members can be selected for policy-based backup and recovery operations. Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB). Once activated, vApps and their virtual machine members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console. As part of this service, VMware will: •Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features. •Perform routine configuration, maintenance and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.	

	•Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment. •Guarantee storage locality per geographical region for all backup data. •Provide necessary Data Protection service reporting as it is requested. Participating entities will be responsible for: •Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements. •Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods. •Registering and unregistering individual vApps and their virtual machine members for scheduled backups using Data Protection. •Performing any on-demand backups per vApp and its virtual machine members. •Performing in-place or out-of-place restores per vApp and/or individual virtual machine. •Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level. •Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMwareTM and deleting any backup data in inventory to free up space.
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.
VirtueStream	Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process. Virtustream provides OS level files are protected with a File System backup and then protect the application with an integrated solution. Some of the databases would dump to a flat file format and those files would be protected with the standard file system backup.

b. Method of server image backups

CA	APM	N/A
	MAA	Automation tools are used to manage the configuration of MAA internal servers, and can be used for recovery.
	CA Agile	Systems are not backed up as we have determined rebuilding is faster than restoring. We manage systems through Chef and the configuration cookbooks are backed up.
	ASM	Automation tools are used to manage the configuration of ASM internal servers, and can be used for recovery.
Virtru	All images are backed up onto cloud storage on two separate provider systems	
Salesforce	Each server has been allocated a different volume group so it can fail over to its backup server within the instance independently of the others.	
ServiceNow	Please see our response to 8.8.2a	
QTS	Your data storage requirements are growing exponentially and a scalable comprehensive solution for storage and data protection is absolutely necessary in today's marketplace. Implementing and managing this necessary storage infrastructure to meet both your application and compliance requirements can be extremely time consuming and costly. Outsource your storage needs to QTS. With our portfolio of high-performance and cost-effective managed storage services, your data will be secure and guaranteed to be available when you need it. By leveraging market leading hardware and software, coupled with certified processes and personnel, QTS delivers dependable, auditable solutions.	

<table>
<tr><td></td><td colspan="2">Managed SAN (Shared and Dedicated)- a fast, reliable Fibre Channel (FC) and iSCSI SAN attached storage solution that easily scales to meet your business requirements.

SAN-to-SAN Replication - provides block level asynchronous replication of your Managed SAN FC service between two of our state-of-the-art data centers for your disaster recovery needs.</td></tr>
<tr><td rowspan="3">SAP</td><td>Ariba</td><td>See above</td></tr>
<tr><td>Fieldglass</td><td>Fieldglass does not run server image backups. All systems are designed to be created through a series of templates and scripts.</td></tr>
<tr><td>Hanna</td><td>The defined backup package includes a file system, operating system files, and the database backup. The frequency in which the backup is executed varies for each of the components mentioned above. This depends on the standard HEC service schedules and the service levels agreed on with the customer.</td></tr>
<tr><td>VMware</td><td colspan="2">VMware will provide the following services to participating entities with respect to Data Recovery:
•Data protection, such as routine backups, for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware.
•Data and infrastructure restoration for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware.
Participating entities will be responsible for the following services with respect to Data Recovery:
•Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air virtual machine's or storage devices, configuration settings, etc.
•Data, content, virtual machine and configuration restorations for assets accessed or stored on your vCloud Air account.
Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important virtual machine data and content hosted in your vCloud Air IaaS environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their virtual machine members can be selected for policy-based backup and recovery operations.
Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB). Once activated, vApps and their virtual machine members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console.
As part of this service, VMware will:
•Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features.
•Perform routine configuration, maintenance and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.
•Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment.
•Guarantee storage locality per geographical region for all backup data.
•Provide necessary Data Protection service reporting as it is requested.

Participating entities will be responsible for:
•Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements.
•Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods.
•Registering and unregistering individual vApps and their virtual machine members for scheduled backups using Data Protection.</td></tr>
</table>

	•Performing any on-demand backups per vApp and its virtual machine members. •Performing in-place or out-of-place restores per vApp and/or individual virtual machine. •Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level. •Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMwareTM and deleting any backup data in inventory to free up space.
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.
VirtueStream	OS level files are protected with a File System backup and then protect the application with an integrated solution where available. Otherwise databases would dump to a flat file format and those files would be protected with the standard file system backup. Additionally, core microVM's are automatically replicated to a secondary datacenter for DR purposes.

c. Digital location of backup storage (secondary storage, tape, etc.)

CA	APM	Backups are securely replicated to an alternate location (within the same geographic location (e.g. N. America))
	MAA	Daily differential and full backups reside in the primacy site with weekly data backups residing offsite.
	CA Agile	Backups are stored in our warm data center.
	ASM	CA has an alternate site approximately 900 miles from our primary site.
Google	Tape	
Virtru	All backup storage is hosten in two separate cloud storage regions	
Salesforce	Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.	
ServiceNow	Please see our response to 8.8.2a	
QTS	Managed Tape Rotation and Off-site Storage This service provides off-site storage for data backup, and helps many customers who must store data separately from a primary IT site to comply with various laws and regulations. QTS has contracted Iron Mountain — a nationally recognized leader in off-site data storage services — to move the data storage media (tapes) to and from a secure, off-site location. The service enables data security, integrity, and restoration in the event of an outage. Off-site data storage via tape ensures that a customer's information is securely stored in multiple locations. In the event of an emergency, QTS and Iron Mountain deliver the customer's media back to their IT environment or wherever they request delivery. Secure: QTS staff adheres to storage-industry best practices and security procedures. QTS facilities have earned SSAE16-SOC1 accreditations. All media is maintained in a secure environment and locked in secure media containers during transition from the QTS environment to the off-site storage location. Compliance and Tracking: QTS's partnership with Iron Mountain provides the ability to offer logging and tracking information about the customer's off-site media via the SecureSync Web portal.	
SAP	Ariba	See above

	Fieldglass	Fieldglass houses all backup data vaults within its production data centers. Replicas of the vault are performed continuously across data centers more than 1,000 miles apart.
	SuccessFactors	All data is backed up to the secondary site and can be restored from there in the event of a disaster recovery event at the primary site.
VMware	VMware vCloud Air Data Protection provides backup storage to disk	
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.	
VirtueStream	Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process. Backup data is stored on local enterprise class disk storage systems and can be replicated to systems in a secondary Virtustream datacenter. All of Virtustream backup is disk based solution. Encryption keys are generated at the time of backup application install on the Client VM(s). Encryption keys are at least AES-128 but can be AES-256. Keys are stored on the backup system databases using the encryption key management tool, the data about the keys on the database is in a unreadable format and cannot be decrypted	

d. Alternate data center strategies for primary data centers within the continental United States.

CA	APM	The location where data is stored is generally in the country where the contract is executed.
	MAA	The MAA service is currently available from one data center only.
	CA Agile	We have a hot/warm data configuration with both data centers located within the US but ~1300 miles apart.
	ASM	ASM has a warm standby with near time data replication between the data centers.
Google	Google does not use the N+1 data center assignment due to the risk of cascading failures. Google's infrastructure makes a dynamic decision for each unique login session which data center is the closest, most highly available data center and which data centers will be used as secondary and tertiary. This assignment would shift for that session throughout the day based on availability and is done completely seamless to the end user.	
Virtru	We utilize multiple availability zones in AWS, and backup all data stored in our database to separate datacenters	
Salesforce	Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location.	
ServiceNow	Please see our response to 8.8.2a	
QTS	The QTS cloud alternate storage sites are located at the following data centers: Richmond, VA, Atlanta, GA, and Suwanee, GA. The entire QTS cloud is a unified standalone Active cloud architecture and is backed up in both Atlanta and Richmond to include: Customer data in the Service Delivery Hypervisor Cluster, and; Cloud Hypervisor Management Infrastructure and Configuration backups.	

	The QTS cloud Security documentation is backed up in alternate site located Suwanee, GA to include: Software/operating Systems, Configuration Data and Security Documentation QTS cloud Management Infrastructure and Configuration Data: Richmond, VA: The Richmond Cloud Management Layer (Cloud Hypervisor Management Cluster) and Customer data in the Service Delivery Hypervisor Cluster, and Configuration data is backed and staged locally in Richmond on the management layer then backed up across the Site-to-Site Management VPN to Atlanta, GA. This process is separate and independent of the Customers Service Delivery Layer. Atlanta, GA: The Atlanta Cloud Management Layer (Cloud Hypervisor Management Cluster) and Configuration data is backed and staged locally in Atlanta on the management layer then backed up across the Site-to-Site Management VPN to Richmond, VA. This process is separate and independent of the Customers Service Delivery Layer. This process maintains both local and remote management layer data and configuration backup for both locations. Suwanee, GA: software/operating systems, configuration data and security documentation at Rocstor Rocsecure Amphibious X7s with Secure-Encrypted Two-Factor Authentication, Utilizing AES-256 CBC Real-Time Hardware Encryption, with NIST and FIPS 140-2 Certified Cryptographic Modules, in a firerated safe located at Suwanee, GA.	
SAP	Ariba	We have a warm site for failover. Equinix (Our primary data center) is located in San Jose, California and our disaster recovery site is located at CenturyLink Data Center in Sterling, Virginia. The act of failing over from the main data center to the recovery site data center has a design goal recovery time objective (RTO) of four hours. The design goal Recovery Point Objective (RPO) is five minutes. In the event of a fail-over to the disaster recovery site location, all URLs that customers use to reach the San Jose data center will continue to work. We will notify customers via their email addresses in the event of unplanned downtime. Internally, we use a documented system recovery plan that outlines the approach and steps for recovering the applications. The document defines roles and responsibilities in the event of disaster: Local staff maintains the hardware remotely We maintain the application software Processes are in place to keep database and fileservers in sync between primary and backup data centers In the event of a catastrophe, we will declare the primary data center ""down"" and our local staff will follow a script to start the applications at the remote data center We test power outage backup scenarios and the Disaster Recovery Plan on a periodic basis.
	Fieldglass	Please see the answer to Question 8.8.2A. above. Fieldglass' backup data center is located in San Jose, CA.
	Hanna	The backup of SAP systems in HEC is executed on EMC DataDomain deduplication storage. This is done using EMC Networker for backup and administration. The backups on Site A are also replicated to remote Site B. For example, site A &B may be Santa Clara, CA and Sterling, VA, respectively.
	Hybris	In the case of catastrophic failure to your primary production data center, we offer anywhere from best efforts to enhanced DR solutions. Enhanced DR

		options translates to either RTO of 8 hours and RPO of 1 hour for a warm standby solution, or RTO of 30 minutes to RPO of 30 minutes for a hot-site. Customers have 3 choices in DR sites: • as part of our base offering, best effort DR, we would bring your site back up in an alternate datacenter which is a minimum of 500 miles away from the primary datacenter. We would actually push your project server images to the alternate datacenter, but we would still need to set up your various interfaces, 3rd party services, etc, which could day a few days. • 2nd would be to have your DR site managed by hybris Managed Services. • 3rd would be to use your own DC as a DR site, We would need to set up a technical call with our combined teams to synch up on the replication strategies. • Our DR services utilizes VMware Site Recovery Manager with storage-based replication. • For enhanced DR, we would include one annual DR test, but more can be added if required. It also includes a customer specific DR and Business Continuity plan.
	SuccessFactors	Each client has a designated primary and backup data center which is geographically separated as well as existing on different power and telecommunications grids.
VMware	Customers can purchase Rackware to provide geographical HA and COOP, but this service is not provided as a core capability of vCA or vCGS. VMware AirWatch AirWatch backs up the production environment from the primary US data center to the secondary US data center. Due to FOIA restrictions and the competitive nature of the EMM landscape, we cannot provide additional backup scheduling or image security procedures.	
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.	
VirtueStream	State of Utah can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01. The State of Utah solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, State of Utah's production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target Recovery Point Objective (RPO) is 30 minutes for virtual machines with a 2 hour Recovery Time Objective (RTO). All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Enterprise Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers. Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process.	

8.9 Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

CA	APM	All data is encrypted via TLS Mutual Auth during transit

	MAA	HTTPS/TLS encrypts the data in-transit. Sensitive data rest is encrypted using native encryption of SQL and NoSQL vendors.
	CA Agile	All data in transit is encrypted - we support TLS 1+. For data at rest we have both database and disk level encryption. DB encryption utilizes Oracle TDE w/ AES-256.
	ASM	All data transmitted between data centers is encrypted in-transit. HTTPS/TLS is used by the ASM dashboard and API.
Google	All connections from customer end point devices to Google's Front End Servers are encrypted with enforced HTTPS sessions using Forward Secrecy. Google websites and properties use robust public key technologies: 2048-bit RSA or P-256 ECDSA SSL certificates issued by a trusted authority (currently the Google Internet Authority G2). All data in transit between Google's Data Centers traverses across Google's private fiber network using a customized, proprietary encryption technology. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. These methods of encryption are fully managed by Google and Google's Key Management Servers based on 128-bit or stronger Advanced Encryption Standard (AES). Encryption Keys and Ciphers Supported by Google Protocols TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.04 QUIC Cipher suites ECDHE_RSA with AES ECDHE_RSA with 3DES ECDHE_ECDSA RSA with AES RSA with 3DES Signing keys RSA 2048 ECDSA P-256 Hash functions SHA384 SHA256 SHA1 MD5	
AODocs	All data in transit is encrypted via SSL/TLS Vendor interfaces are available only via HTTPS Email is exchanged via SMTP/TLS All AODocs data are stored in Google AppEngine.	
Virtru	AES-256 in CBC mode, TLS 1.2 ECDHE	
Salesforce	Encryption Capabilities Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their	

	respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements. Data In Motion All transmissions between the user and the Salesforce Services are TLS encrypted with a 2048-bit Public Key. The Services use International/Global Step Up TLS certificates, with AES 256-bit encryption by default. Data At Rest Salesforce includes a feature to encrypt custom text fields (ECF): The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number). Access to read the masked parts of the fields is limited by the ""View Encrypted Data"" permission, which is not enabled by default. Customers can manage their encryption key based on their organization's security needs and regulatory requirements. Encrypted fields are encrypted with 128-bit keys and use the AES (Advanced Encryption Standard) algorithm. Additional Salesforce Encryption Capabilities Apex Code extends the powerful and proven success of the Force.com platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, your Agency can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. Third Party Encryption Solutions (Additional License Option) Should additional encryption be required, third party solutions such as CipherCloud, Skyhigh, and PerspecSys are available on the Salesforce AppExchange. These solutions offer data loss prevention, user activity and monitoring, malware protection, as well as data protection with encryption and tokenization. Data can be encrypted and masked at rest, keys managed and stored in Salesforce, and compliance controls to prevent unauthorized access to data and keys.
ServiceNow	ServiceNow makes use of encryption for both data in transit and data at rest. ServiceNow provides optional capabilities with regard to the encryption of data at rest within the system, which customers can apply at their own discretion. Encryption in Transit ServiceNow customers access their instances over the Internet using forced Transport Layer Security (TLS) encryption (AES128/256) for all user access. The level of encryption is based on the browser and must be configured by the customer as ServiceNow does not modify any browser settings. All attempts to access ServiceNow over HTTP are redirected to HTTPS. Integration Encryption For integrations such as LDAP and Web Services, ServiceNow provides customers with the ability to encrypt traffic. LDAP can be configured to run over SSL, this requires customers to provide a certificate for the specific LDAP server. Certificates may also be stored within an instance to allow encrypted transmission for Web Services integrations. FTPS and SCP can be used as file transfer methods to securely transfer files to ServiceNow. Email Encryption Customers may configure their instance to generate emails to their users from the instance. ServiceNow provides the capability to receive email over TLS. Customers are able to configure their

	email system to send email to ServiceNow over TLS and ServiceNow will receive that email over TLS. Encryption at Rest ServiceNow can provide three types of encryption for data at rest that are implemented by the customer or by customer request in the case of edge encryption and dedicated hardware. •Column encryption of customer added fields and attachments: Provides data encryption using AES128/256 or 3DES symmetric key encryption. The customer provides the keys for this encryption. Data stored in these fields cannot be searched or reported on and this does not support out of the box fields. •Edge Encryption Proxy: With optional additional cost Edge Encryption, the customers create and control their encryption keys within their own network. Edge Encryption includes a proxy application that resides in a customer's network. This encrypts data before it is sent (also encrypted in transit) from the customer's environment to the ServiceNow instance. The data always remains encrypted whilst stored in the instance and the data along with the keys and the encryption configuration is never accessible by ServiceNow. Requests for encrypted data must also be made through the proxy application and is therefore decrypted only within the customer's network before being sent to their end users client browser. Please note that data encrypted with Edge encryption cannot be used by back-end scripts or processes and searching and reporting behavior is also modified through its use. •Full disk encryption: Provides via self-encrypting hard drives with AES256 bit encryption. This encryption capability is only available through the purchase of dedicated ServiceNow hardware at an additional cost. This delivers "at-rest" protection only and is focused solely on preventing data exposure through the loss or theft of hard disks holding customer data. Wherever possible, ServiceNow leverages existing FIPS 140-2 certified technologies.	
Docusign	Secure, private SSL 256 bit viewing session Anti-tampering controls Signature verification of signing events Unalterable, systematic capture of signing data Digital certificate technology Customer configurable data retention program	
SAP	Ariba	We enforce minimum AES 128-bit encryption using Transport Layer Security (TLS) for all sessions. We encrypt only PCI-DSS data in the database where appropriate and in support of PCI-DSS compliance. All backup media is encrypted using AES 256-bit cipher prior to transporting to off-site storage
	Fieldglass	Our application provides a high level of application-level security through a combination of encryption, page-level access checking, document envelopes, and activity logging. Application security is handled through a combination of programming checks, application server configuration, and database server configuration. Fieldglass uses 2048-bit SSL (HTTPS) encryption for all data transmissions over the public Internet, including data shared between the product and end users and data shared between the product and back-end systems. Data is decrypted on the internal VLAN to allow IDS monitoring. Passwords are hashed using a one-way hash based on the SHA-256 encryption algorithm. The hash value is saved within the database; not the password. The base Fieldglass application does not require data that would require breach notifications if compromised. While customers should not store sensitive personal data, custom fields may be defined by the customer that can be encrypted with AES-256 to capture any pertinent and permissible data points. These fields can also be optionally masked from view while entering and viewing the fields in the application.

	Hanna	Initial encrypted data load - physical encrypted data transfer possible Encrypted connection to HEC DC - SAP solutions support various VPN-device vendors and specifications that can be used to setup a secure and encrypted tunnel between cloud solutions from SAP on the customer network segment and the customer site. Optional Data at Rest encryption - HANA encryption at Rest activated during system build upon request. Moreover data at rest is properly protected against unauthorized access, these controls include •Physical security controls in SAP HEC Datacenters in place •Physical separation of "online" storage and backup (physically separated DC sections) •Strict User and Access Management (segregation of duties) •Authorization Management according to the need to know principle also for administrative accounts, e.g. DBAs have limited authorizations to perform DB operation only •Security Logging and Security Monitoring for critical activities / access Optional encryption in transit can be configured on customer request which requires a different subset of DC's from delivery perspective.
	Hybris	Encryption is provided through SSL connectivity at the web application layer as well as VPN secure encrypted tunnel for back-office integration connectivity. Further encryption capabilities are available through the hybris Advanced Security Module (optional).
	SuccessFactors	All data in the system is treated as highly sensitive information. The application and infrastructure offers Strong Encryption, Encryption in Transit and Encryption at Rest, including the following (some of these are options that are not included in the base services): Transport Layer Security (TLS) technology, consisting of a public key and a private key, to protect sensitive information. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a handshake authenticates the server (website) and the client (browser). An encryption method is established with a unique session key. Customers may then begin a secure session that facilitates message privacy and integrity. Hitachi SAN storage arrays provide a reliable safe, secure data storage environment. We use AES-256 bit encryption to secure data at the block level of our storage systems. Backups are performed ""disk to disk"". Data is transported over 3DES VPN and stored on encrypted disk using Data Domain replication technology
VMware	VMWare IaaS Services Data in transit will be encrypted based upon the customers selected method of transport (SSL or IPSEC VPN). Data at rest encryption is the responsibility of the customer. By example HyTrust is an endpoint encryption choice for many vCloud Air customers. VMWare AirWatch AirWatch leverages strong, non-proprietary encryption algorithms to protect applicable data at rest and in transit. Due to FOIA restrictions and the competitive nature of the EMM landscape, we cannot provide specific encryption algorithms and protocols.	
FireEye	Each of the FireEye offered solutions have their own implementations and practices concerning encryption:	

	1.Email Threat Prevention (ETP) ETP offers TLS encryption support for data in transmission. ETP only stores email found to contain malware or malicious content and does not encrypt this data. 2.Mobile Threat Prevention (MTP) All data in transit is protected using standard TLS encryption. The database itself is not encrypted. However, all systems are under strict security and access control rules, in compliant with SOC 2 regulations. 3.Threat Analytics Platform (TAP) All data in-transit between a customer environment and TAP instance in Amazon AWS is encrypted with a 256-bit Twofish key. No customer data is stored on disk, however data stores leverage Amazon AWS S3 encryption settings. 4.FireEye as a Service (FaaS CV) FireEye appliance communications, and FireEye as a Service (FaaS) non-person entity (NPE) secured inter-process communications employs industry standard HTTPS encrypted web interfaces, and multifactor SSH management access for the end-to-end protection of sensitive customer data. In addition, FaaS communicates with FireEye appliances with additional layers of protected symmetric key exchanges protecting and establishing encrypted channels for inter-device information.
VirtueStream	Encryption keys are generated at the time of backup application install on the Client VM(s). Encryption keys are at least AES-128 but can be AES-256. Keys are stored on the backup system databases using the encryption key management tool. The data about the keys on the database is in an unreadable format and cannot be decrypted.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Carahsoft would be willing to sign Business Associate Agreements or similar agreements that are set forth with a purpose of protecting customer data.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Agreed and understood. Carahsoft and its' subcontractors will not use any government data for purposes other than those outlined within the frameworks of this contract.

8.10 Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

CA	APM	The target availability SLA of 99.8% is standard and not negotiable
	MAA	The target availability SLA of 99.8% is standard and not negotiable
	CA Agile	The target availability SLA of 99.8% is standard and not negotiable
	ASM	The target availability SLA of 99.8% is standard and not negotiable
Google	Google maintains a single SLA for all customers.	
AODocs	AODocs maintains a single SLA for all customers.	
Virtru	Agreement can be negotiated for certain large customers.	

Salesforce	Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status. Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.	
ServiceNow	ServiceNow's SLA is not negotiable. ServiceNow delivers the same level of world-class support to all customers as described in the "Subscription Service Guide" included with this response. ServiceNow's homogeneous private cloud environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow. ServiceNow's experience & understanding of its private cloud and the benefits provided by a consistent infrastructure and standardized processes allow it to provide a high level of security, availability, and performance in a cost effective and reliable manner.	
Docusign	Yes SLA's can be modified per contractual agreement.	
SAP	Ariba	Our SLAs are not negotiable. As mentioned above, the SAP Ariba Cloud Service Level Agreement includes a 99.5% uptime.
	Fieldglass	Our SLA is designed to (i) meet the expectations of our customers and (ii) fit with our operational protocols and capabilities. Because of this our ability to make significant changes to the SLA is limited. However, we are always willing to work with a customer to try and determine how our SLA can address a particular business.
	Hanna	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a future invoice relating to Cloud Service that did not meet the System Availability SLA.
	Hybris	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a

		future invoice relating to Cloud Service that did not meet the System Availability SLA.
	SuccessFactors	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a future invoice relating to Cloud Service that did not meet the System Availability SLA.
VMware	VMware's SLAs are specific to the product or service, and are subject to the product's Terms of Service (which are also provided). The SLA is specific to the product rather than to the customer, to define the expected availability and recourse should the product not meet the stated availability levels. VMware's existing customers include Federal, State and Local government customers as well as commercial customers, who successfully utilize our products in accordance with the current SLA and Terms of Service and their applicable, mandatory laws and regulations. Accordingly, VMware is confident that the existing SLA meets the state and local government requirements, as it is being utilized currently. VMware IaaS Services To best work with our customers and improve our terms in alignment with market requirements, VMware is willing to review the terms of its SLA during negotiations of the Participating Addendum to identify how the existing SLA meets the state's applicable and mandatory laws and regulations. If it becomes apparent to the parties that it is necessary to revise VMware's SLA to comply with the state's applicable and mandatory laws, VMware will enter into discussions about how to best address these requirements Vmware SaaS Services VMware AirWatch AirWatch Service Level Agreements are non-negotiable. AirWatch has a guaranteed uptime SLA of 99.9%. Please refer to the AirWatch Hosted Services Policy for additional information. VMware AirWatch acknowledges that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the mandatory minimum requirements and technical specifications of the RFP.	
FireEye	SLAs are negotiable.	
VirtueStream	Virtustream's Service Level Agreement is generally not negotiable. Our SLAs are one of the strictest in the market place. To change the SLA would mean either changing the design or create operational disruption and higher cost by engaging in non-standard processes and practices. For example, Virtustream's SLA for Tier 1 storage is 10 ms latency. For Virtustream to change this latency means changing the design for Tier 1 storage.	

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Below is a sample of Virtustream's Service Level Agreement:

SERVICE LEVEL FRAMEWORK
The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.
Commencement of Service Levels
Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services

does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

Service Level Review Meetings

Monthly Service Level review meetings will be conducted by Virtustream with Customer where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a.Promptly investigate and report on the causes of such problem;

b.Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c.Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d.Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e.Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f.Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

a.A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b.Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

c.Any hardware, software or other product of a third-party or Customer equipment;

d.Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

e.Downtimes resulting from a Virtustream's scheduled maintenance windows;

f.Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

g.Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;

h.An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a µVM pool that is insufficient to run the designated workload);
i.Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;
j.Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply;
k.Resolution delays due to lack of client response and/or Customer provided credential based information;
l.Priority levels not agreed upon by both customer and supplier;
m.Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

8.11 Data Disposal

Specify your data disposal procedures and policies and destruction confirmation process.

The disposal of data will vary based on the type of service that is being provided to the Purchasing Entity by Salesforce. As an example, please see Salesforce response for disposal of government data: Data Disposal and Destruction
In the event of termination of the Salesforce service, requests by your Agency made within 30 days after the effective date of termination or expiration of the Subscription Agreement, Salesforce will make your data available to you for export or download. Once the export has been completed, an email will be sent to you containing a link where you can download a .zip file that contains multiple .csv (spreadsheets) files, each representing your Salesforce objects. Your data on disk is flagged within the database and set to inactive status or what can be referred to as a ""soft delete."" This data is no longer available or accessible to the application but is backed up in the full database backup process. The data remains in this state for 180 days; this is done in the event that the customer decides to resume services or needs the data for a legal reason. At 180 days, the data is marked for deletion (""hard delete"") and will be deleted after 30 more days. Once this ""hard delete"" is executed the customer data is physically deleted and non-recoverable from the database. Following the purge, the data will remain on backup for an additional 90 days prior to being overwritten and unrecoverable.

Media Sanitization
Salesforce has an established process for sanitizing media consistent with industry guidelines and consistent with NIST SP 800-88 Guidelines for Media Sanitization [MP-6].

8.12 Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

CA	APM	CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.
	MAA	CA MAA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.
	CA Agile	For Rally SaaS Unlimited Edition customers, our goal is to provide 99.9% up-time during each calendar quarter. If in any calendar quarter an up-time of 99.5% is not met and our customers were negatively impacted (for example, were unable to login to Rally), we will provide a service credit equal to one month of fees for use of the Rally Service.
	ASM	CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.

Google	Google Apps services will be operational and available to the customer at least 99.9% of the time in any calendar month. If Google does not meet the Google Apps SLA, the customer will be eligible to receive service credits.	
AODocs	Altirnao agrees to use commercially reasonable efforts to meet or exceed the Availability Service Level. The Availability Service Level means the Service is available for use by Users for not less than 99.5% of the time excluding the Exclusion Events (as defined below).	
Virtru	Virtru provides the same SLA as Gmail	
Salesforce	Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent. Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.	
ServiceNow	ServiceNow's Availablity SLA Is 99.8%, excluding Excused Downtime of up to two hours per month. This is achievable through the use of the Advanced High Availability (AHA) architecture described in 8.8.1 that provides failover capabilities for maintenance and service disruptions to minimize downtime.	
Docusign	DocuSign offers carrier class bank grade, "always on" availability. This means DocuSign has eliminated monthly maintenance (taking 0 minutes of planned downtime per year). We are a multi-year 99.99% operation. Please view the DocuSign Trust site (trust.docusign.com) for additional information.	
QTS	TIA 942 requirements for the design, construction, and management of Tier III facilities is the design basis for all QTS data centers. Using best-of-breed technologies, QTS's highly trained, certified data center professionals tailor efficient and reliable solutions to meet individual customer requirements. Primary commercial power is delivered to facilities through diverse, redundant paths to eliminate single points of failure between the nearest electrical substation (usually on-site) and each piece of customer IT equipment. QTS allows users to inspect the engineering drawings to validate that truly redundant N+1 architectures are in place and that the 99.999% uptime guarantee is supported by sound engineering and operational policies. Meaningful Service Level Agreements are backed by financial penalties spelled out in tailored Master Service Agreements with each customer.	
SAP	Ariba	Our data centers have 99.99% uptime. Our application maintains a 99.% official SLA with the last 12 months seeing 99.98% uptime.
	Fieldglass	For customers hosted in US data centers, we commit to a 99% availability standard. For customers who choose to be hosted in EU data centers, our availability standard is 96.7%. If we fail to meet the availability standard, the

		customer may be entitled to receive a credit equal to two percent (2%) of its transaction fees for the service for that month for each one percent (1%) (or portion thereof) by which we fail to achieve such level, up to one hundred percent (100%) of the fees for such month.
	Hanna	The SAP HEC offers a 99.5% uptime availability SLA for production (PRD) instances and a 95% uptime availability for quality assurance (QAS) and development (DEV) instances. This means that after taking in to account the monthly maintenance window, the TOTAL solution will be available 99.5% of the time - not that we expect it, but this equates to about 3 hours of unscheduled downtime per month. The concept of "total solution" is important because the HEC provides Holistic Solution Availability - our single SLA covers the FULL SOLUTION STACK which means it covers the Infrastructure, Operating System, local DB, the HANA in-Memory DB, and the Application layers. We do not offer individual SLAs on individual layers because if one layer fails, the entire solution is down
	Hybris	The environment is completely redundant and based on a high availability architecture. The hybris private cloud is based on VMWare virtualization and is fully load-balanced. Customer systems reside on a redundant server infrastructure ensuring that if one server (or part of the server infrastructure) fails, a backup is in place to ensure that systems remain operational. The infrastructure is load-balanced ensuring high availability of the system during peak usage periods. The load-balancing allows the systems to support large volumes of simultaneous users balancing the load of activity across multiple servers ensuring peak performance of all systems. Redundancy of Infrastructure Components: • Multihome connectivity to the Internet backbone. Multiple connections to the internet, allows optimizing the best route as well as redundancy. • At an individual component level, all devices have dual physical power connections to protect against any individual power supply failure • Redundant Firewalls • Redundant Routers, • Redundant Load balancers • Virtualized Application and Web servers • Clustered Database - active active cluster mode for enhanced redundancy • High performance SAN storage- from Netapp, with built in redundancy at the disk level (NetApp proprietary RAID technology, similar to a RAID 5) • The data centers provide diverse power (Uninterruptible Power Supply), backup generators and air conditioning systems required to ensure equipment remain online with optimal performance 24/7/365. • SLA: contractually we provide a guarantee on the performance of your application at 99.9% availability.
	SuccessFactors	We contractually guarantee a minimum of 99.5% system uptime, with the exception of regularly scheduled and emergency maintenance.

VMware	VMware's SLAs for vCloud Air. Our Availability Commitment ranges from 99.99% - 99.95 based on the Class of Service. The SLAs are subject to the terms of the applicable Terms of Service for the VMware vCloud Air Service Offerings. Dedicated Cloud 99.99%, Virtual Private Cloud 99.95%, Data Protection 99.95%, Disaster Recovery 99.95%, Virtual Private Cloud On-Demand 99.95% Availability Commitment. IaaS Object Storage: Object Storage powered by Google CLoud Platform (standard) 99.9%, Object Storage powered by Google (durable reduced availability) 99.0% and Object Storage (nearline storage) 99%. vCloud Government Service Dedicated Cloud 99.95% and Virtual Private Cloud 99.9% Availability Commitment.
FireEye	FireEye undertakes all reasonable efforts to ensure the availability for 99.9% of the time during each calendar month. In the event the solution does not meet the monthly service availability, FireEye will provide a credit as outlined in the SLA.
VirtueStream	Virtustream solution for VM workload includes the uptime of 99.99%.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

CA	APM	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
	MAA	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
	CA Agile	See above.
	ASM	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
Google	Google Cloud Platform SLA: Google's Cloud platform has SLAs ranging from 99.9 - 99.95% uptime.	
Salesforce	Please see response to 8.12.1 above. Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published.	
ServiceNow	DEFINITIONS (a) "Available" means that the Subscription Service can be accessed by authorized users.	

	(b) “Excused Downtime” means: (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow’s control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow’s direction, a Force Majeure Event, general Internet outages, failure of Customer’s infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks. (c) “Maintenance Time” means the time the Subscription Service is not Available due to service maintenance. (d) “Availability SLA” means the percentage of total time during which Customer’s production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime. AVAILABILITY If Customer’s production instances of the Subscription Service fall below the Availability SLA of ninety-nine and eight-tenths percent (99.8%) during a calendar month, Customer’s exclusive remedy for failure of the Subscription Service to meet the Availability SLAs is either: (1) to request that the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or (2) to request that ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per minute rate ServiceNow charges to Customer for Customer’s use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees. REQUESTS Customer must request all service credits or extensions in writing to ServiceNow within thirty (30) days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer’s production instances of the Subscription Service was not Available. The total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for the month, and has no cash value. ServiceNow may delay issuing service credits until such amounts reach one thousand U.S. dollars ($1,000) or equivalent currency specified in the applicable Order Form.	
Docusign	Our industry-leading, global support model is there to back you up, no matter where you do your business. We provide you access to the expertise you want, whether through our communities, our knowledge base and on-demand training, or our team of experienced technical support professionals, who know you and your solutions.	
QTS	99.999% uptime guarantee. Meaningful Service Level Agreements are backed by financial penalties spelled out in tailored Master Service Agreements with each customer.	
SAP	Ariba	We guarantee a 99.5% system availability percentage during each month for production versions, with the exception of regularly scheduled and emergency maintenance.
	Hanna	Technical Availability for PRD systems - 99.5% Technical Availability for non PRD systems - 95% SAP shall track and report to Customer the “Technical Availability” in a monthly summary report. SAP HEC can offer a contractual SLA of 99.7 on a case by case basis.
	Hybris	SLA: contractually we provide a guarantee on the performance of your application at 99.9% availability.

	SuccessFactors	We guarantee a 99.5% system availability percentage during each month for production versions, with the exception of regularly scheduled and emergency maintenance.
VMware	AirWatch Service Level Agreements are non-negotiable. AirWatch has a guaranteed uptime SLA of 99.9%. Please refer to the AirWatch Hosted Services Policy for additional information. VMware AirWatch acknowledges that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the mandatory minimum requirements and technical specifications of the RFP.	
FireEye	FireEye cloud solutions are available 99.9% of the time in any calendar month, other than mutually agreed upon and scheduled downtime.	
VirtueStream	Virtustream IaaS Compute is comprised of computing resources hosted in secure data centers that replace the physical computing hardware traditionally housed on Customer site. These resources include physical servers which are logically divided into VMs (virtual machines), each with an allocation of CPU and memory, and linked to storage. Terms used in the detailed descriptions below: •µVM. Pronounced "micro VM," this is Virtustream's fine-grained unit of measurement designed to accurately measure the actual consumption of cloud resources. A µVM is a unit of computing resources, comprised of CPU, memory, storage IOPS, and associated local network bandwidth. The usage of each µVM resource component (CPU, memory, storage input/output, and network bandwidth) is measured at five minute intervals — one unit each for 200MHz of CPU, 768MiB of memory, 40 storage fabric input/output operations per second (IOPS), and 2Mbps of local network bandwidth. The highest of the four is averaged per hour, and the hour values averaged across the month to determine the overall µVM usage for the month. Note: The measurement is performed at the aggregate level — across Customer's entire µVM resource pool. Bandwidth usage is only within the data center. •Basic Plus uVM. These terms differentiate the two ways Virtustream offers µVMs services. "Basic Plus" µVM services are limited to a single Virtustream data center and have 99.99% availability for the Customer's committed level. "Reserve" µVM service is an equivalent quantity of Basic Plus µVMs reserved at Customer-designated secondary Virtustream data center for on-going operation during disaster events and during scheduled disaster recovery (DR) exercises. In both cases, overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level. •High Memory. Virtustream offers competitive pricing on compute services for applications that require large amounts of memory (64GiB or more). •Enterprise These terms identify the "zones" within which µVMs are made available for consumption. The "Enterprise" zone is for use by non-Internet facing workloads. Systems deployed into the Enterprise zone are not directly accessible from the Internet. Enterprise Basic Plus µVM (IC-uVM-BASP-ENT) Enterprise Basic Plus µVMs reside in a single Virtustream data center, in the Enterprise zone. Resource availability is 99.99%, and only at the designated data center. Overage resources required ("surges") up to 20% above the committed level from the contract /order form is provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level. Service Level. 99.99% availability for the Customer's committed level. Billing. Monthly, based on resource usage. Tier 0 Block Storage - Local Only (IC-STO-TOA-LOC) Block storage with a Latency Service Level of 3ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.	

	Tier I Block Storage - Local Only (IC-STO-T1A-LOC) Block storage with a Latency Service Level of 10ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier II Block Storage - Local Only (IC-STO-T2A-LOC) Block storage with a Latency Service Level of 20ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier III Block Storage - Local Only (IC-STO-T3A-LOC) Block storage with a Latency Service Level Objective of 40ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier 0 Block Storage - Replicated (IC-STO-TOA-REP) Data storage with a Latency Service Level of 3ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier I Block Storage - Replicated (IC-STO-T1A-REP) Data storage with a Latency Service Level of 10ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier II Block Storage - Replicated (IC-STO-T2A-REP) Data storage with a Latency Service Level of 20ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier III Block Storage - Replicated (IC-STO-T3A-REP) Data storage with a Latency Service Level Objective of 40ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

CA	APM	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per

		day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
	MAA	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
	CA Agile	Support is available 24/7 and a contact number will be provided upon completion of the contract.
	ASM	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
Google	Customers are entitled to direct Google support in additional to whatever Support Services the reseller has to offer. Google has a published Technical Services Support Guide for both Google Apps and Google Cloud Platform that describe the hours of operation, how to get after hours	

	support, how to set the priority on a case, how to contact Google, and what the target response times are.
AODocs	Customers are entitled to direct AODocs support in additional to whatever Support Services the reseller has to offer.
Salesforce	Salesforce is proposing the Premier+Success Plan. Your Agency can cover all of its bases with this plan: support, training, and administration. It's what the + is all about. The Premier+ Success Plan gives you all the benefits of our Premier success plan, including a support rep assigned to your organization, priority case routing, 1-hour response time, 24x7 phone support, unlimited usage of our entire online course library, plus one very helpful addition: access to your own team of expert Salesforce administrators. This lets you focus on design and management while we support your configuration. The Premier+ Success Plan includes: ● Unlimited access to our entire online course catalog of 100+ courses ● 24x7 toll-free phone support ● Priority case queuing and routing ● Quick 1-hour response time ● An assigned support account rep ● Force.com code troubleshooting ● Customizable end-user course templates ● Premier Success Review to measure usage and trends ● Access to our pool of Salesforce Certified Administrators who can configure and maintain your Salesforce edition ● Premier Success Review to measure usage and trends ● Includes administration services: Get configuration help. Request 100+ routine configuration updates like creating users, reports, workflow, and dashboards. You take online administration training to learn the basics, then you tell us your business requirements. Our team of certified administrators updates your Salesforce system. Subject to the Government Cloud Premier+ Success Plan outlined above, access to systems and permissions which could permit access to Customer Data inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC Customer Data will be restricted to Qualified U.S. Citizens. Qualified US Citizens are individuals who are United States citizens, and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce.Severity Levels & Response TimesIssues will be categorized and handled according to an assigned severity level, as follows: Level 1 - Critical Response time: 1 Hour* Critical production issue affecting all users, including system unavailability and data integrity issues with no workaround available. Level 2 - Urgent Response time: 2 Hours* Major functionality is impacted or significant performance degradation is experienced. Issue is persistent and affects many users and/or major functionality. No reasonable workaround available. Also includes time-sensitive requests such as requests for feature activation or a data export. Level 3 - High Response time: 4 Hours**

	System performance issue or bug affecting some but not all users. Short-term workaround is available, but not scalable. Level 4 - Medium Response time: 8 Hours** Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Reasonable workaround available. Resolution required as soon as reasonably practicable. *24/7 Severity 1 and 2 coverage includes weekends and holidays **Severity 3 and 4 target response times include local business hours only and exclude weekends and holidaysOverview of Support Escalation PathAn issue is received by Tier 1 Support Rep who will document details and attempt to resolve. In the event that the problem cannot be resolved at this level, case will be escalated to a Tier 2 Support Rep for further analysis. Occasionally, a Case may be received for which technical understanding or indicated fix exceeds the responsibility of Support. These issues are quickly brought to the attention of R&D through the Tier 3/QA channel. Throughout the lifecycle of the case, customer will receive regular updates from the case owner at regular intervals based on case severity. Customers can work with their Support Account Specialist (SAS) if assigned through the purchase of Premier Support as a point of escalation should the need arise. Step-by-step escalation path: •Case is logged via Help Portal, Phone or through Live Chat •Depending on the functional area of the case a Tier 1 Support Rep from the appropriate skill group responds to the user confirming that the issue has been received and is in process. •Tier 1 analyzes the issue from the perspective of customer provided information in the case. •Tier 1 makes contact (phone or email) with the customer and gathers more information including any access needed to reproduce the problem. •With all necessary information gathered, Tier 1 will attempt to resolve the issue with the customer. •When resolution cannot be immediately achieved, Tier 1 Support Rep will escalate to a Tier 2 Support Rep in the same skill group. Tier 2 Support Rep will take all steps necessary to reproduce, understand and resolve the issue. •Technical Issues that cannot be resolved by the Tier 2 Support Rep are escalated to Tier 3. This escalation will provide a deeper layer of analysis with the possibility of escalation to QA/Development for Application issues and Escalation to Operation Services for Infrastructure issues as needed. •Functional Issues that cannot be resolved by Tier 3 are escalated to Product Management. •If it is an application Issue, necessary Development work will be performed, tested and a patch created. •Issue Fix Submitted to Operations for Infrastructure issues. •Issue Fix deployed. •Tier 2 Support Rep confirms success of Bug Fix in addressing the problem. •Tier 2 Support Rep contacts customer and confirms that the issue is Resolved. •Case is closed"
ServiceNow	Customer Support is provided by ServiceNow 24 hours a day, 7 days a week, including all holidays. Customer may contact ServiceNow using one of the following means: •Support Portal at https://hi.service-now.com/. Customer may get login access to this self-service portal by contacting its ServiceNow administrator. •Phone using one of the numbers at http://www.servicenow.com/support/contact-support.html. Customer shall contact ServiceNow's authorized reseller in accordance with its agreement with the reseller.

	See the "Customer Support Policy" contained within the "Subscription Service Guide" included with this response for more information.
Docusign	Enterprise Premier support provides 24x7 Live Phone Support.
QTS	Dedicated support staff is available 24x7x365 to generate and track incidents to resolution QTS Customer Portal provides round-the clock visibility into your environment
VMware	Global Support Services
FireEye	FireEye offers 24/7 technical support and its technical support centers around the globe in a follow-the-sun model. •Milpitas, CA, USA (UTC -7 hours) •Reston, VA, USA (UTC -4 hours) •Dublin, Ireland (UTC) •Singapore (UTC +8 hours) •Sydney, Australia (UTC +10 hours) FireEye Support is available via telephone, email, live chat, and web. Phone: U.S: +1 877-347-3393 (877 FIREEYE) Email: Support@FireEye.com Web Support: https://www.fireeye.com/support/get-support.html Support Programs: https://www.fireeye.com/support/support-programs.html
VirtueStream	Virtustream will work collaboratively with State of Utah to develop / maintain a relationship structure that leads to quick resolution, regularly scheduled status meetings, and quarterly business reviews. Virtustream will assign multiple key personnel to State of Utah including an Executive level sponsor. The primary point of contact will be Virtustream's Technical Account Manager (TAM). The TAM is responsible for daily activities/interaction and understanding/ensuring State of Utah's objectives are met at a minimum. Optimizations and other improvements to processes/standard operating procedures are delivered by the TAM in coordination with other Virtustream staff working behind the scenes. The TAM will coordinate day-to-day operation, service level management and SL reporting. The following outlines Virtustream's approach to service desk escalation and issue resolution. Escalations within Virtustream Virtustream will provide Level 0 and Level I support and first call resolution where possible, as determined by Virtustream. Where first call resolution is not possible, the Virtustream Service Desk provides incident management for Incidents and Urgent Service Requests escalated to Level II and Level III resources as defined below. In the event that Virtustream's Response to an Incident is not acceptable to the Customer, Customer can contact the Virtustream Service Desk and request escalation to the head of the Service Desk. Virtustream shall, upon receipt of any such request, immediately escalate the issue to the head of the Service Desk or technical team as appropriate. Service Request Prioritization Service Requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All Service Requests will be reviewed by the Virtustream Service Desk, who will determine the appropriate priority to assign with collaboration of Customer. Incident Prioritization All Incidents that are reported to the Virtustream Service Desk, or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream Service Desk as set forth below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Incident Prioritization			
Priority/ Severity	**Definition**	**Response Time Service Level**	
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. **Or** Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	**30 minutes**	Response time will be within indicated time beginning from when the customer creates a ticket or a monitoring event is validated. Additional resources are engaged via Virtustream's on Call Process.
2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. **Or** Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	**60 minutes**	
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. **Or** Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	**4 hours**	
4	Incident that is causing inconvenience to the business, but not impacting operations. **Or** Incident has a minor impact on users or business, or issue is a request for further information	**1 business day**	

Virtustream will assign a Technical Account Manager starting on day 1 of the contract. The Cloud Platform, Cloud Cover (managed services), and Cloud Security team's will also be assigned to State of Utah upon execution of the contract. All of the individuals assigned to the State of Utah account have significant years of experience in their fields.

The TAM assigned to State of Utah will provide reports ad hoc but also on a quarterly basis. The quarterly business reviews include but are not limited to performance measurements, service requests. On a monthly basis, the TAM will provide a consumption report detailing the items consumed by each virtual machine. This delivers a very granular cost breakdown to State of Utah which will allow the data to be carved multiple ways. Also, information can be gathered by the State of Utah team any time they want from the xStream portal. State of Utah can also issue a ticket to Virtustream operations center to request information as well. The TAM will conduct scheduled meetings and be in constant contact with State of Utah. The TAM is an extension of the State of Utah team.

Virtustream defines a Root cause analysis (RCA) as the formal process, documented in writing by Virtustream and approved by Customer, to be used by Virtustream to diagnose problems at the lowest reasonable level which includes a report of the corrective action to be taken and defined timelines for corrective actions, which shall eliminate, to the extent reasonably possible, repeat failures. The following details the RASCI for RCA's:

	Role/Function	Customer	Virtustream
	Request Root Cause Analysis tickets by contacting the Virtustream TAM (Customer requests Incident report/Problem record)	R/A	S
	Document, track and manage all Problem tickets using ITSM system	S	R/A
	Provide Problem management review and Root Cause Analysis (RCA) for all in-scope P 1 Incidents (preliminary report within 48 hours; final within 15 calendar days)	S	R/A
	Provide Problem management and RCA of identified Problems (e.g., reoccurring events, alerts) - investigate and diagnose	S	R/A

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

CA	APM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the contract.
	MAA	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the SaaS Listing.
	CA Agile	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the contract.
	ASM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the SaaS Listing.
AODocs	If AODocs does not meet the SLAs, the customer will be eligible to receive a service credit.	
Virtru	Email support@virtru.com	
ServiceNow	ServiceNow or its authorized reseller, as applicable, will use reasonable efforts to meet the target response times and target level of effort stated in the "Customer Support Policy" contained within the "Subscription Service Guide" included with this response for more information.	
SAP	Ariba	As part of the Cloud subscription, Ariba provides Customer Support services to help diagnose, troubleshoot and resolve functional and technical problems for all users. Ariba's award winning customer service staff can be contacted via phone (toll free), email or Web form Monday-Friday, 24/5 in multiple time zones and languages. Ariba Connect, our online support portal provides 24/7 support for service and enhancement requests. Customers may also choose to purchase ExpertCare. ExpertCare provides each customer with a named contact within Ariba that acts as an ExpertCare Manager for the customer and is knowledgeable about customer specific business process, configurations and customizations.
	Fieldglass	Our best practice is that the program office (managed by the State of Utah or your chosen MSP) provides first-level support for end users including hiring managers, approvers, suppliers, etc. Fieldglass' multi-lingual helpdesk is available by phone, email or web form 24x7x365. Our English language helpdesk is located at our corporate headquarters in Chicago. Merlin Information Systems Ltd., a UK entity, provides helpdesk service in French, German and Japanese from its Manila,

		Philippines and Debrecen, Hungary locations. We are prepared to assist with technical, functional or administrative questions about the Fieldglass application.
	Hanna	Customer key users have several options to communicate incidents into SAP Managed Cloud Delivery. Primary entry point: The best and easiest way to get an incident resolved is by creating and sending incidents directly to SAP Managed Cloud Delivery Service Teams via the SAP Support Portal. This communication channel ensures that all support teams are notified and therefore is the most preferred way to contact SAP on support/service related issues. Alternative option to the primary entry point: Customer key user can also communicate incidents by telephone via the SAP Customer Interaction Center (CIC) (e.g. in case of facing challenges in submitting an incident via the SAP Support Portal). Exceptional option: During business hours, customer key user may also communicate urgent incidents by contacting designated SAP Managed Cloud Delivery service contacts like Customer Engagement Service Manager (CESM) to create an incident on behalf of the customer. However – as already mentioned - this is not the preferred way of communication, but only should be applied in exceptional cases. Support times are contractually agreed upon with each individual customer organization. The SAP Managed Cloud Delivery (MCD) Service Desk and the Service Teams are spread across Europe, Americas and Asia.As a result of the global set-up across several time zones, SAP MCD Service Desk is able to provide worldwide 24/7 support to customers, throughout the entire year and according to the “Follow-The-Sun-Principle”.
	Hybris	Key service levels are delivered through service level objectives, which provide for uptime of 99.9 for the hosted environment. Furthermore, monitoring is in place to report and alert upon uptime and response times of the environment to ensure best possible performance. The following support is specifically for the SAP Hybris Commerce, Cloud Edition. Customers can contact SAP Hybris Commerce, Cloud Edition technical support by toll-free telephone number or e-mail 24 hours per day, seven days per week. Based on the priority level, SAP Hybris’s support personnel will attempt to provide Customer with remote assistance for reported issues. Contact information for technical support is as follows: Toll-Free Telephone Number: 888-944-2664 ext 6 In the event that Customer contacts SAP Hybris support, SAP Hybris shall respond to such reports as follows: Priority Level : Characteristics Response Time Resolution Time Objective

		Priority Level 1 Fatal Issue: Problem causing the Customer Website to cease from operating. This situation is generally described as a total failure. 25 Minutes (7x24) 2 hours Priority Level 2 Major Issue: Problem causing the Customer Website to experience major problems with it ability to operate. This situation exists when the Customer Website is partially failing however it is still able to function. 25 minutes (7x24) 12 hours Priority Level 3 Degradation of Performance: Problem affecting only certain non-critical functions of the Customer Website. This situation is occurring when the Customer Website is usable but has certain limited functions. 2 hours 1 business day Priority Level 4 Minor Issue: This situation includes all other non-critical problems. It is present when the Customer Website is usable however the problem results in a minor issue affecting it. 2 hours 3 business days Upon receipt of a service call classifying the priority level, SAP Hybris will deploy commercially reasonable efforts to respond and assist in the resolution of the problem. Application support for code developed by Customer or its implementation partner will be provided by Customer or Customer's implementation partner. If SAP hybris provides SAP Hybris Commerce, Cloud Edition support to a Customer as requested by Customer, and it is subsequently revealed that SAP Hybris was not responsible for the problem or the problem was not classified correctly by the customer, Customer will pay SAP Hybris on a time and materials basis for such support and assistance.
	SuccessFactors	
VMware	Our Availability Commitment for VMware AirWatch is 99.9%. The SLAs are subject to the terms of the applicable Terms of Service for VMware AirWatch. If the Availability of a class of service that you purchase is less than the associated Availability Commitment, then you may request Service Credits for that affected class of service. Availability in a given month is calculated according to the following formula: "Availability" = ((total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month) x 100 A class of service will be considered "Unavailable," subject to the Service Level Agreement Limitations set forth below, if VMware's monitoring tools determine one of the following events has occurred ("SLA Event"). The total minutes that a class of service is Unavailable for a particular SLA Event is measured from the time that VMware validates the SLA Event has occurred, as defined below, until the time that VMware resolves the SLA Event such that the Service Offering is Available to you. If two or more SLA Event occurs simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.	

	1. Each of the following will be considered an SLA Event for the Dedicated Cloud, Virtual Private Cloud, or Virtual Private Cloud OnDemand Services: a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. The "Service Offering Network" means the network that extends from the network interfaces of physical host servers for a class of service to the outside network interfaces providing the Service Offering's public internet connectivity. b) The data store(s) associated with your block level storage for a class of service are unavailable for more than three (3) consecutive minutes. c) The self-service console, available at https://vchs.vmware.com, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes. d) Your running virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures. 2. Each of the following will be considered an SLA Event for the Data Protection Service: a) The backup storage repository associated with your Data Protection service is unavailable for more than three (3) consecutive minutes. b) The start time associated with your backup scheduling window is missed for longer than thirty (30) consecutive minutes. c) The standard 24-hour recovery point objective (RPO) is missed for any virtual machines actively enrolled in the service. d) Any restore operation for a virtual machine fails to complete due to backup infrastructure failures. 3. Each of the following will be considered an SLA Event for the Disaster Recovery Service: a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. b) The data store(s) associated with your block level storage for replication is unavailable for more than three (3) consecutive minutes. c) The self-service console, available at https://vchs.vmware.com, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes. d) Your failed-over virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures. e) Any built-in service functions for failover testing, planned migration, or live failover and recovery result in virtual machine replicas not powering on in less than 4 consecutive hours from the time a request is acknowledged and approved by VMware. 4. The following will be considered an SLA Event for the Object Storage service: a) A more than five (5) percent Error Rate for more than ten (10) consecutive minutes – where "Error Rate" means the number of valid requests that result in a response with HTTP Status 500 and Code "Internal Error" divided by the total number of valid requests during each five-minute period.
FireEye	FireEye shall use commercially reasonable efforts to correct any reproducible programming error in the Software attributable to FireEye, employing a level of effort commensurate with the severity of the error, provided, however, that FireEye shall have no obligation to correct all errors in the Software.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

CA	APM	Planned downtime is scheduled, and customers are notified
	MAA	Customers are notified at least two weeks in advance for planned downtime.
	CA Agile	Regularly scheduled maintenance (planned downtime for upgrades and maintenance) where the customer has been given at least eight (8) hours notice does not count as downtime. Unscheduled maintenance, in which the Rally Service is unavailable and

		advance notice was not provided to customers, will be counted against the up-time SLA.
	ASM	Customers are notified at least two weeks in advance for planned downtime.
Google	Google's maintenance routines are done in a manner that ensures there is no need to schedule any downtime.	
AODocs	AODocs's maintenance routines are done in a manner that ensures there is no need to schedule any downtime.	
Salesforce	There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance. System Maintenance is for sustaining the performance, reliability, security, and stability of the infrastructure supporting our services. When maintenance is scheduled, the specific timing and availability to be expected during that time will be communicated to all customers approximately one week in advance of the maintenance window upon login to Salesforce and via a posting to http://trust.salesforce.com/trust/maintenance. In the event of planned maintenance where the services will be unavailable for more than four hours, or that requires customer action in advance, Salesforce endeavors to communicate via email several months in advance. Please Note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance. Major Release Maintenance is for upgrading the services to the latest product version to deliver enhanced features and functionality. Major release dates and times are posted on http://trust.salesforce.com/trust/maintenance approximately one month before release to Sandbox instances. An email notification and blog post regarding Sandbox preview instructions is also sent approximately one month prior to upgrading Sandbox instances. Email notification of major release dates is sent one month prior to upgrading non-Sandbox instances. The Release Notes document describing the new features and functionality is posted in Help & Training one month prior to upgrading non-Sandbox instances. Final release reminders are communicated to all customers approximately one week prior via email and upon logging into Salesforce. Major release maintenance occurs three times per year. The instance will be unavailable for up to five minutes during the release window. Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime.	
ServiceNow	ServiceNow notifies customers at least 10 days prior to scheduled maintenance for infrastructure network, hardware or software that might impact service. ServiceNow targets no more than two hours of downtime due to scheduled maintenance per month.	
Docusign	Continuous availability is a necessity for mission-critical business applications in a global world. It's also a key component of the xDTM standard. Zero maintenance downtime means that DocuSign is always available, regardless of the time-of-year, day-of-week, time zone or country. DocuSign's Carrier Grade System Architecture, a first in SaaS, eliminates maintenance downtime, and ensures the highest level of performance resiliency and data integrity. This is accomplished through a combination of advanced high availability architecture, native DocuSign engineering, and both specialized and commodity hardware and software components.	
SAP	Ariba	Scheduled downtime windows for maintenance, upgrades or new releases are provided in the Service Level Agreement. Our uptime percentage takes scheduled maintenance into account.

	Fieldglass	Fieldglass' maintenance windows are as follows: • Friday maintenance window of 11:00 p.m. – 2:00 a.m. Central (Daylight Savings Observed) • Extended maintenance windows are taken with five days advance notice and are typically as follows: - Second Friday of each of the following months: March, July, and November - Critical service packs, security issues, and other emergencies will still be taken if needed with communication as reasonable
	Hanna	SAP performs periodic scheduled maintenance activities to maintain security patching levels, application transports, fixes, network maintenance, and other scheduled proactive activities during scheduled maintenance window (agreed to by the customer). The predefined maintenance window is 4 hours per month (for example first friday of every month) SAP may perform additional maintenance services on the Customer's Computing Environment in agreement with Customer, with at least ten (10) Business Days prior notice (which notice may be by email to Customer's nominated contact or posting) of the date and anticipated length of the maintenance window, and provided that SAP adheres to Customer's reasonable requirements as to the timing and duration of any such maintenance. SAP reserves the right to apply critical application and operating system security patches in compliance with the SAP Global Security Team's reasonable recommendations. SAP will use reasonable endeavours to provide Customer with forty-eight (48) hours advance notice regarding the critical patch deployment unless a shorter notice period is required in order to address a critical security issue. Non critical security issues shall be dealt with by Scheduled Maintenance
	Hybris	Typically they are two-hour maintenance windows, with no downtime or on occasion maintenance periods require between 2 to 10 minutes of downtime. Other rare periods which may require further maintenance could have downtime between 30 min to 4 hours.
	SuccessFactors	To address issues such as security patches, hot fixes, updates, equipment upgrades, etc., we has established maintenance windows to perform scheduled maintenance. Scheduled maintenance events typically occur during only one of these windows, roughly every 6-8 weeks. A 14-hour/week window will be used for all critical / most emergency patches and all bug fixes (will include tech stack and application patch sets). We define scheduled downtime maintenance windows as: Midnight to 7 a.m. Fri-Sat local time + midnight to 7 a.m. Sat-Sun local time (dependent upon the data center where the customer data is hosted) We will provide customers with at least a 2 days' notice if a larger maintenance window is needed. Typically, for HCM / LMS products, customers receive a 3-5 day notification (via popup on login). When the system is not available during the maintenance there is a notification page displayed for the outage timing. We plan maintenance events conservatively, and use them sparingly.
VMware	VMware IaaS Services Customers are notified in advance of any expected downtime with vCloud Air services. In the event of an unexpected outages or disruption to the service, customers will be notified via their preferred contact means as soon as possible as per the terms outlined in the Service Level Agreement. VMWare AirWatch	

	We maintain standard SLAs with our customers to provide for downtime • SLAs are defined within the AirWatch Hosted Services Policy Per our Hosted Services Policy, we provide outage credits in the event of a service interruption: • ""AirWatch warrants it will provide Availability of the Hosted Services 99.9% of the calendar month (the "Service Level"). To the extent that the Hosted Services fail to conform to the Service Level, Customer may request service credits ("Outage Credits") as provided herein. A failure or lack of Availability for any period of time of at least one minute during which Customer is unable to utilize the Hosted Services due to AirWatch's failure to provide Customer with the specified services constitutes an "Outage". All Outage measurements will be rounded up or down to the nearest one minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Outage Credits are based on cumulative periods of Outage over a calendar month. Final determinations of the length of the cumulative periods of Outage over a calendar month shall be based on AirWatch's internal monitoring equipment and records. Outage Credits will be taken against only the Hosted Service fees for the month in which the Outage occurred.""
FireEye	FireEye undertakes reasonable efforts to ensure that the service availability maintains a minimum of 99.9% availability. However there are circumstances where the system will be down due to the following: a) "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer. Customers receive notification and announcements for any scheduled maintenance period. b)"Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance.
VirtueStream	Virtustream planned downtimes start with the weekly change board meeting by the Platform Operations group. All requested changes whether requested by customers or by the operations staff are reviewed, if approved then scheduled. Depending on the nature of the change, routine and planned, the affected customers are notified as early as possible and adjusted based on customer needs. For example, if the scheduled downtime falls on a weekend that a customer plans to do their quarterly close, Virtustream will reschedule. An emergency/urgent change may have less notice for the customers. But in all cases, customers will be notified of the upcoming downtime multiple times, start of the downtime will be specified and the expected duration. Once the downtime is complete, another notification will go out to the affected

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

CA	APM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in contract. Defined, monetary penalties are provided in the SaaS Listing document.
	MAA	Defined monetary penalties are provided in the SaaS Listing document
	CA Agile	See 8.12.4
	ASM	Defined, monetary penalties are provided in the SaaS Listing document
Google	Customers will be eligible to receive a service credit.	
AODocs	Customers will be eligible to receive a service credit.	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at primary data center facility without stopping access to the application.	

	For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency. In terms of remedies, the Salesforce Service Terms incorporated as part of the End User Licensing Agreement indicate the following regarding Termination allowing customers to terminate the contract at time of renewal: ""User subscriptions will automatically renew for additional periods of one (1) year at the list price in effect at the time of renewal unless You give Your Reseller notice of termination at least 30 days prior to the end of the relevant subscription term.""	
ServiceNow	See 8.12.2 for the Availability SLA.	
Docusign	See 8.12.4.	
SAP	Ariba	Please see the details provided in 8.12.4 response.
	Fieldglass	Please see the answer to Question 8.12.4, above.
	Hanna	Penalties and remediation for SLA violations are detailed in the Statement of Work.
	Hybris	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
VMware	For VMware there is a service credit reimbursement structure outlined above. We have detailed recovery procedures that include defined steps, roles and responsibilities and accountable personnel to help ensure streamlined disaster recovery. As conversations progress, AirWatch can provide specific details regarding our disaster recovery timelines and strategies.	
FireEye	FireEye has established formal Business Continuity and Disaster Recovery plan, as well as Incident Response and Recovery Plans to help maximize availability of critical customer-impacting services.	

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

CA	APM	A report of the Service's measured monthly SLA is available to Customer upon request
	MAA	Reports are generated periodically and ad hoc. Customers can use their support.ca.com credentials to access private trust site which contains SLA details for the subscribed service.
	CA Agile	Realtime and historical system status can be viewed at https://status.rallydev.com
	ASM	Reports are generated periodically and ad hoc.
Google	Google does not produce customer specific performance reports. The web based Apps Status Dashboard displays real time System Availability Details. Customers can works with their Google reseller to design a reporting system using Google Sheets based on which incident actually impacts their end users. Service availability issues are isolated to specific applications and specific geographically locations and thus would not impact all of your users or your account at all.	
AODocs	AODocs does not produce customer specific performance reports. Customers can visit the AODocs status page: status.aodocs.com. AODocs provides a set a usage reports and AODocs team can also work with the customer to build specific reports	
Virtru	We have realtime monitoring of both server side operations and client side interactions.	
Salesforce	System Performance ReportsOur track record speaks for itself—Salesforce has maintained high levels of availability across all Salesforce instances since inception. As an on-demand vendor	

	providing daily service-quality data on a public website (http://trust.salesforce.com), Salesforce proves that it is a leader in availability. And by making its track record completely transparent, salesforce.com proves it is worthy of customers' trust. A few metrics that we maintain (and publish publicly via our trust.salesforce.com website) are: -Daily Transaction Counts -Daily Transaction Speeds Salesforce is hitting almost 4 billion transactions a day. These transactions are a mix of user interacting with the system and API calls where other systems are bi-directionally interacting with Salesforce. Our Average Transaction Time hovers between 150 and low 200 milliseconds. Some additional published metrics are uptime & availability, planned maintenance windows, and any performance degradation. The Purchasing Entity can view all of this information and more by going to trust.salesforce.com. Customers can also log a case to request system uptime reports for the last 6 months and last 12 months, however, system reports are not automatically distributed.	
ServiceNow	Administrators can view a wide range of performance metrics for their instance and for the machine on which the instance is running, displayed in a graphical format. Add these graphs and their controls to a home page to monitor the performance of instances. Some of these graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues or help tune your system for maximum efficiency. Each graph enables admins to filter the data by using different measurements, such as maximum and minimum values, means, and medians. The available graphs reflect performance in eight functional areas of ServiceNow. •Database •Discovery •Disk Partitions •Linux Stats •Logging •MySQL Overview •Node Metrics •Replication •ServiceNow Servlet	
Docusign	For real-time data, please visit the DocuSign Trust site (trust.docusign.com) for additional information.	
SAP	Ariba	We provide a monthly report to customers describing the system availability percentage. Depending on the cloud service, these reports are made available either by email, through the cloud service or through an online portal.
	Fieldglass	Fieldglass executes comprehensive performance testing prior to each release to production. Performance testing is executed in accordance with the Fieldglass Performance Testing Standards document. Types of testing performed include regression, load, stress, and endurance. Results are reviewed and approved by senior members of development, QA, IT, and the Chief Architect. Our standards document can be shared upon request while under NDA. During peak periods, Fieldglass will see 12,000 concurrent users with page response times averaging 400-700ms. Across all of 2015, we have a 99.4% success rate in meeting or exceeding all monthly customer SLAs for page response times.
	Hanna	Performance reports on HEC are available to the customer via the SAP One Portal page. It provides the customer among other things: operational info about systems being managed, incident management, security management, user specific settings, planned downtime, etc.

	SuccessFactors	Customers can view hosting performance and availability information real-time at the following link: https://support.successfactors.com/Service_Status.
VMware	VMware IaaS Services VMware vCloud Air provides Web-based capacity reporting via the MyVMware portal. For detailed performance reporting, participating entities may wish to acquire VMware vRealize Operations suite, which is a non-Web based software product which provides real-time and historic performance statistics for vCloud Air. VMWare AirWatch We can provide sample performance testing documents that validate our ability to handle anticipated workload under real-world conditions as conversations progress. We have a dedicated team for scalability and performance testing. They work with both internal teams and customers to conduct testing.	
FireEye	This is not applicable as each of the FireEye offerings are classified as SaaS. The performance of the FireEye cloud environments are continuously monitored and managed by the cloud service operations (CSO) team to ensure secure operation and availability.	
VirtueStream	Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.	

8.12.8 Ability to print historical, statistical, and usage reports locally.

CA	APM	A report of the Service's measured monthly SLA is available to Customer upon request
	MAA	Same as above.
	CA Agile	This is available upon request.
	ASM	Customers are sent monthly SLA reports.
Google	See 8.12.7	
AODocs	See 8.12.7	
Virtru	We may be able to publish reports locally for customers.	
Salesforce	Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find: ● Live and historical data on system performance ● Up-to-the minute information on planned maintenance ● Phishing, malicious software, and social engineering threats ● Best security practices for your organization ● Information on how we safeguard your data	

	In addition to the Salesforce Trust site (http://trust.salesforce.com/trust/status) to monitor uptime and performance, your Agency will also have access to a System Overview, which will help you monitor performance and usage of your own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used License Usage API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages Portal Usage The above list is of all the possible metrics that you may have in your system overview.	
ServiceNow	Yes. Instance performance can be viewed locally. Customers can use the Customer Support Portal to obtain information about the real availability of all their instances. Real availability is the percentage of production time that an instance is up and available for use.	
Docusign	Yes. DocuSign offers a number of pre-defined reports to provide detail and summary information on DocuSign usage in the account, such as by Envelope, Recipients, Velocity of signing, and User Access among many other reports. Users can modify report criteria such as data ranges and reports can be scheduled to execute. All reports can be downloaded or Printed locally.	
QTS	Yes	
SAP	Ariba	User access is browser-based, so printing is enabled via the printers that are setup on the user's workstation. There are several "Print" buttons throughout the applications that will open an additional browser window with a printer-friendly format of the screen.
	Fieldglass	Any user with the correct permissions in the system, as specified by the State of Utah, may locally print historical, statistical, and usage reports.
	Hanna	Yes, available
VMware	VMware IaaS Services At the present time, VMware does not provide end user customers with specific reports for SLA performance. VMware tracks the overall health of the environment and will report to customers in the event of an outage. However, specific SLA performance is not delivered as a report, but as an alert. It is currently the customer's responsibility to track downtime within their environments and report to VMware when they believe SLA has been violated. VMWare AirWatch Customers can export and print solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV)	
FireEye	Each of the offerings in this response have reporting capabilities local to the system and users with the appropriate access rights.	

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

CA	N/A. CA only offers SaaS solutions and manages all aspects of the service. Clients do not have direct access to the environment.
Google	Purchasing entities will subscribe to an initial set of user licenses and can provision new user accounts at their convenience within that range of licenses.
Salesforce	The Salesforce service can be deployed rapidly since our customers do not have to spend time procuring, installing or maintaining the servers, storage, networking equipment, security products,

	or other infrastructure hardware and software necessary. The service is always available and the customer can deploy 24x365 at their own pace.
ServiceNow	ServiceNow is supported 24x365.
FireEye	The FireEye offerings in this response are SaaS service models. Once the application or service is set up there are no further deployment steps necessary. On-demand Self-service options referenced in section 8.1.2.1 are available 24x365.
VirtueStream	Virtustream's self-service portal allows authorized users to deploy resources on-demand 24x365.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

CA	N/A. CA only offers SaaS solutions and manages all aspects of the service; monitoring and capacity planning is included as part of the service.
Google	Purchasing entities will subscribe to an initial set of user licenses and can provision new user accounts at their convenience within that range of licenses. If the purchasing entity has exceeded or is about to exceed their user count they can place an order for additional licenses at any time. Scale-down procedures will be handled on the renewal anniversary.
Salesforce	The Salesforce cloud based architecture will allow the State to deploy Salesforce solutions rapidly and scale at will for future needs. Customer's may scale up and add licenses at any point during their annual contract cycle. User counts are examined on an annual basis at time of renewal to ensure the customer had adequate license coverage.
ServiceNow	ServiceNow can automatically scale its application servers horizontally by adding or subtracting them to the load balancer pools for a particular instance. Scaling is managed by the ServiceNow Cloud Operations team.
FireEye	The FireEye offerings in this response are SaaS service models. FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure optimal resources are allocated to the system 24x365.
VirtueStream	Virtustream's self-service portal allows authorized users to deploy or de-commission resources on-demand 24x365.

8.13 Cloud Security Alliance

Describe your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.
b. Completion of Exhibits 1 and 2 to Attachment B.
c. Completion of a CSA STAR Attestation, Certification, or Assessment.
d. Completion CSA STAR Continuous Monitoring.

Carahsoft is proposing a number of Service Providers that are members of the Cloud Security Alliance. For example Salesforce is a corporate member of the Cloud Security Alliance (CSA) and contributes to their research and initiatives in a variety of ways. Salesforce has completed the CSA Consensus Assessments Initiative questionnaire (CAIQ), which maps to the CSA Cloud Controls Matrix (CCM) for the Salesforce Services, including Force.com, Analytics Cloud, Communities, Chatter, Sales Cloud and Service Cloud. A copy of the current completed CSA CAIQ can be provided to prospects or customers under NDA upon request.

8.14 Service Provisioning

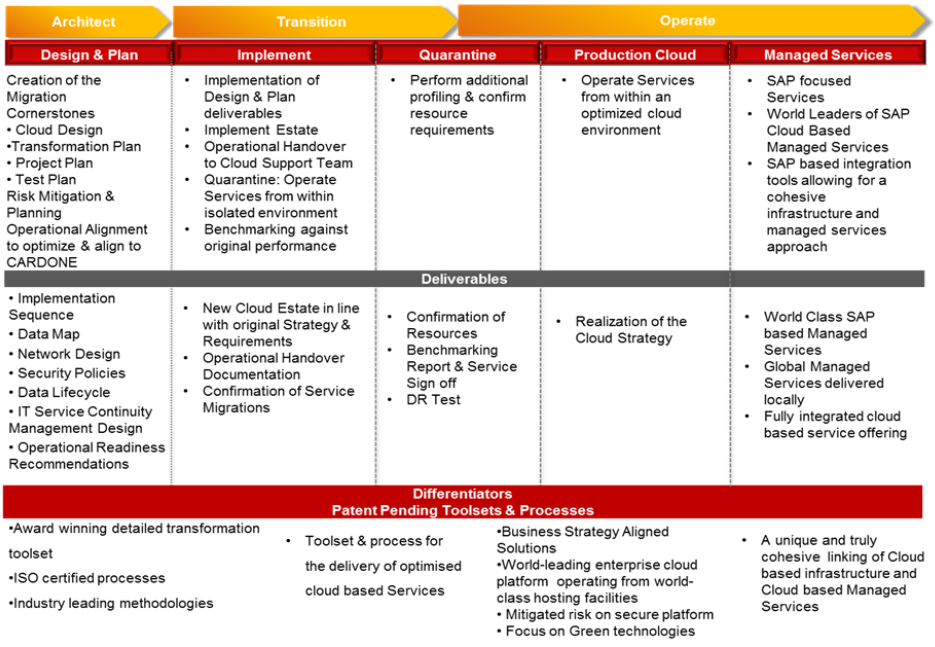
8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

CA	APM	CA SaaS Ops has a rigorous service introduction and update process that is governed by a central body to ensure adherence. Every step in the process is recorded, tracked and approved.
	MAA	Standard lead times for requests can be waived for requests that have a critical business need
	CA Agile	Standard lead times for requests can be waived for requests that have a critical business need such as a data recovery effort
	ASM	Standard lead times for requests can be waived for requests that have a critical business need such as a data recovery effort
Google	Order processing from the time a valid Purchase Order is submitted has a normal turn around time of three business days. Google's sales team can be contacted to expedite orders when needed.	
AODocs	Order processing from the time a valid Purchase Order is submitted has a normal turn around time of two business days. AODocs's sales team can be contacted to expedite orders when needed.	
Virtru	Requests are triaged by the support and if an emergency is identified, the request is escalated by the VP of Product who immediatlye assigns the issue as a top priority to a developer. Once completed a hotfix is pushed to production.	
Salesforce	Subscription-based, On-Demand Service Salesforce offers on-demand Platform as a Service (PaaS) and Software as a Service (SaaS). The Salesforce PaaS and SaaS offerings are subscription based and in a per user/month or user/year format billed annually with some of our products offered as total logins per month or by defined number of members billed annually. Multi-tenancy gives applications elasticity. Force.com applications can automatically scale from one to tens of thousands of users. Processing more than three billion transactions each day, Force.com is used for large-scale deployments. Any application that runs on Force.com is automatically architected to seamlessly scale from 1 user to 100,000 users without the customer having to do anything differently. All applications (includes mobile, offline and read-only options) and data running on Force.com are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization's mission-critical applications.	
ServiceNow	ServiceNow professional services organization responds to customer needs based on each request. Once a purchase order is received from the Purchasing Entity, ServiceNow contacts the Customer to discuss schedules. Resources are assigned based on the project need. If the customer has a priority issue with the system, they would open a ticket and the ticket SLA process would proceed until the issue is resolved. Every ServiceNow customer is supported based on their priority and need.	
SAP	Hanna	Rush or emergency infra provisioning can be request in exceptional situations and would be addressed on best effort priorty basis.
VMware	VMware IaaS Services Initial Order - Expedite the purchasing process thro - In the event that an emergency or rush service implementation request is received, VMware's NASPO program manager will coordinate an expedited response depending on the request. - Expedited Procurement - The Program Manager will directly interface with each company in the supply chain to ensure that the order is processed immediately upon receipt by each party. - Expedited In Increased capacity	

	VMWare AirWatch Participating Agencies will work with thier dedicated Account Executive to procure addition services for thier AirWatch implementations. Customers can implement and update configurations through the AirWatch administrative console. Additionally, customers can submit ASK tickets for any solution issues that will be tracked through completion.
FireEye	FireEye will make every reasonable effort to accommodate rush provisioning requests. The purchasing entity should contact their sales account team who will interface directly with the corresponding implementation team to coordinate an expedited implementation.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

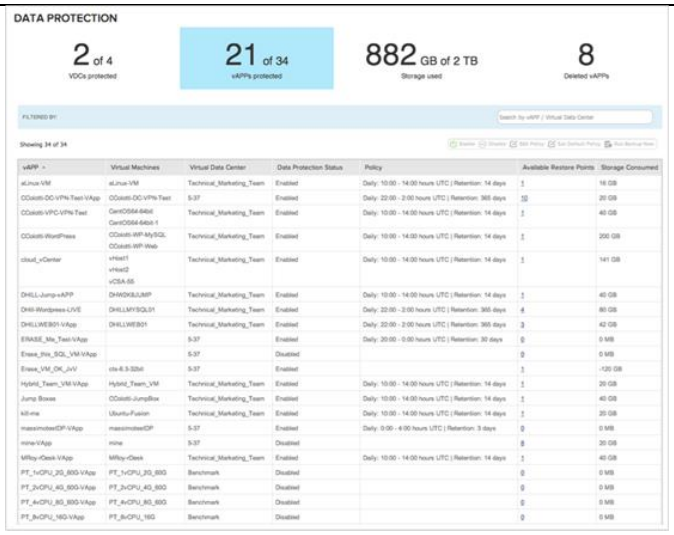
CA	APM	48 hour turnaround is typically required
	MAA	Services do not generally require client action for provisioning. General service catalog requests have a standard 48 hour lead time
	CA Agile	Services do not generally require client action for provisioning. General service catalog requests, such as a data refresh, have a standard 48 hour lead time
	ASM	Services do not generally require client action for provisioning. General service requests have a standard 48 hour lead time
Google	Standard lead time is three business days.	
AODocs	Standard lead time is two business days.	
Virtru	The Lead-time for provisioning is no more than 15 minutes	
ServiceNow	ServiceNow provisions new instances or newly purchased users or applications to the instance within 48 hours after receipt of order. If users or applications are required more quickly, the customer controls access to all ServiceNOw capabilities at any time and the true-up occurs thereafter.	
Docusign	DocuSign is intuitive and easy-to-use. Getting started with our cloud solution, standard console, can be implemented in a day. Adding integrations or API's will add to the complexity of the implementation, but our Professional Services are there to guide you every step of the way.	
VMware	VMware vCloud Air Services VMware vCloud Air OnDemand services can be purchased and provisioned in minutes via the vCloud Air self service portal. VMware vCloud Air services other than OnDemand are purchased via purchase order. Purchase orders are typically processed on the day of order. Once services have been purchased the user can immediately begin provisioning services from the self service portal. These services are available within minutes of launch. VMware vCloud Government Services VMware vCloud Government Services are purchased via purchase order. Purchase orders are typically processed on the day of order. New environments require an RSA token that is overnighted for 2 factor authentication. Once the user has their RSA token they can begin to provision IaaS Services. VMWare AirWatch AirWatch is committed to implementing the solution in a timely manner and we work closely with customers to meet internal deadlines. Delivery and deployment models will vary depending the hosting model selected by the customer: • SaaS deployments can be implemented within several days and some within a few hours • Large enterprise deployments with numerous integration endpoints may require additional time Once an order is placed, we immediately begin working with the customer to finalize terms and conditions in a mutually agreeable manner and begin the implementation process. We schedule regular check-ins for project status updates and to discuss any questions or concerns.	

FireEye	FireEye anticipates that the standard lead-time is expected to take no more than five (5) business days. However, FireEye is willing to accommodate an urgent request from NASPO in order to provide adequate service to the participating states.
VirtueStream	Virtustream's standard lead-time for provisioning can vary based of the type of deployment and requirement. Resources can be deployed on-demand basis by State of Utah. For the initial services, there is a standard which is maintained as best practice. At project kick-off, Virtustream and State of Utah will develop a detailed Implementation Plan, on a system-by-system, week-by-week basis, to ensure that both sides of the relationship have clear expectations on what is to be accomplished, by whom, and in what timeframe. Upon completion of the Implementation Plan, Virtustream and State of Utah will establish a Project Governance Plan and the Project Governance Plan will manage Implementation Plan and ensure alignment at all tiers of the organization, define expectations for status update frequency and formats, and establish an escalation path for issue identification and resolution. Virtustream offers a dedicated onboarding project team that is charged with migrating clients into the xStream® cloud. This chargeable service includes resources from our platform and SAP teams and development of an onboarding project plan with milestones and deliverables. Virtustream uses a mature methodology to move clients onto our cloud platform, a process which is continuously refined and improved. A link is established to the client site using a Virtual Private Network (VPN) or Multiprotocol Label Switching (MPLS) circuit, for customer access and testing of migrated systems. Prerequisites are put into place (domain controllers, backup systems, infrastructure, networking, etc.) prior to systems being onboarded, in a defined sequence. Virtustream SAP basis team members test the systems before turning them over to Ascend for validation. Once on the xStream® platform, Virtustream monitors, backups and maintains the systems. As a component of the Virtustream platform, all core units are replicated to an alternate data center to provide disaster-recovery capability. **Figure 3. Sample Work Plan** 

8.15 Back Up and Disaster Plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

CA	APM	Not currently available.
	MAA	Not Available.
	CA Agile	The customer is responsible for the lifecycle of their data. We will retain all data until it has been deleted from our systems. We can remove data from our systems upon written request from the customer at termination of the contract.
	ASM	Not available.
Salesforce	Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce Services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may schedule a weekly export of data or copy to a sandbox account. Exports of Customer Data are available in comma separated value (.csv) format by request via Salesforce's Customer Support department. In addition, many exports can be manually pulled by the designated org administrators.	
ServiceNow	Once notified ServiceNow has the ability to leverage our internal clone operation process. This provides a locked state copy of the instance, while the customer can continue working on the production instance. Any data additions, changes or deletes will be on the production but not on the frozen instance copy. Additionally, ServiceNow can freeze backups to prevent them from being over written.	
Docusign	DocuSign customers determine their retention policies.	
QTS	Yes QTS will work with customers to meet legal requirements.	
SAP	Ariba	For the network's standard record retention is 180 days, but customers can request longer terms.
	Fieldglass	Fieldglass has many methods in which we can freeze customer data, today. We have the capabilities to restore, utilizing a point in time recovery method to a secondary system for legal review effectively delivering a system that has been frozen in time for all clients.
	Hanna	HEC standard backup retention is 1 month for productive systems, and 14 days for non-productive systems. However retention period can be changed per request and may have cost impact.
	SuccessFactors	A customer can configure as many ""purge rules"" as required to comply with data privacy rules. Since these rules vary by country, the solution provides the flexibility to define different retention periods for groups defined by country, department, division, location, job code and hire date. Customers can grant permissions to the appropriate users to create a request to purge data and to approve the request to purge data. These ""purge rules"" can be scheduled to reoccur. User records are kept in the system, for reporting purposes, but their data is anonymized. Our customers use the solution in compliance with local regulations today in almost 180 countries.
VMware	VMware IaaS Services Participating entities that leverage VMware Data Protection are able to specify the retention period of their backups to comply with policies and legal requirements. Data Protection leverages snapshots to take an image level backup of virtual machines. When a backup is initiated, a snapshot is taken of that virtual machine. Once the snapshot is taken it is then stored on the Data Protection storage for the duration of the retention period assigned in the policy. The policy column in the screenshot below illustrates the variety of data retention policies that have been set within a sample customer's vCloud Air Data Protection instance. In this example retention policies range from 3 to 365 days.	

	 VMWare AirWatch Customers can export and archive solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV). Customers in a Dedicated Cloud deployment can leverage a robust data mart.
FireEye	Customers have access to data stored in the varying cloud solutions and are accessible at any time during the length of the subscription contract. Retention periods vary per service offered. See section 8.7.2 for further information.
VirtueStream	Specific retention requirements can be accommodated on a custom basis. More detailed information would need to be provided in order to scope.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

CA	APM	DR is provided only in a single geography at this point. Professional Services would need to be engaged to provide multi-geo DR
	MAA	N/A
	CA Agile	None - our DR plan is tested at a minimum semi-annually.
	ASM	None
Virtru	Please see the Virtru Disaster Recovery Plan provided in the Supplemental Information section of this response.	
Salesforce	The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location [CP-4, CP-6, CP-7, CP-9, MP-5].	
ServiceNow	ServiceNow is divided into two distinct environments for Business Continuity (BC) and Disaster Recovery (DR). ServiceNow's corporate environment and its data center environments are physically and logically isolated from each other. A disaster in ServiceNow's corporate environment could occur with little or no impact on the ability for the data centers within the private cloud to operate. In both cases, the BC and the DR are supported by a series of SOPs that allow ServiceNow to quickly and effectively take action when it is required.	

<table>
<tr><td></td><td colspan="2">ServiceNow's customer DR is documented in its Information System Contingency Plan (ISCP), which covers its data center environments, and includes all customer environments as well as the instances that ServiceNow uses to run its business.

ServiceNow formally tests this process on an annual basis and can produce compliance reports for customers requiring them. ServiceNow also uses the process of transferring instances to reduce the impact of maintenance on its service and will move instances out of one data center to the other on a daily basis. As a result, ServiceNow is very well practiced at the process of "failing over" customer instances.

ServiceNow's BC process covers its functional offices and is a separate standard operating procedure from its customer environments. The BC Plan (BCP) has been developed in concert with the entire business including Business Impact Assessments (BIA) to understand the impact of the loss of any given systems or locations.</td></tr>
<tr><td>Docusign</td><td colspan="2">DocuSign is dedicated to providing the industry's most secure eSignature solution through the DocuSign Security Assurance Program.</td></tr>
<tr><td>QTS</td><td colspan="2">Not having a current copy of your information.
Mitigation - QTS's DR High Availability Service provides continuous data replication of your physical and virtual server environments, ensuring you always have access to a current copy of your data, applications and operating systems.</td></tr>
<tr><td rowspan="4">SAP</td><td>Ariba</td><td>Ariba has a strong disaster recovery procedure, tested every 6 months though has never required to fail over to the backup data center. The RTO is 4 hours and RPO is 5 minutes. Please see the SaaS Technical Infrastructure Whitepaper for addiitonal details.</td></tr>
<tr><td>Fieldglass</td><td>None.</td></tr>
<tr><td>Hanna</td><td>SAP Hana Enterprise Cloud helps customers improve their Business Continuity requirements with High Availability (HA) , Disaster Recovery & Backup options.
High Availability (HA) - HA is achieved by failover to standby node
Disaster Recovery (DR) - Systems are configured in the secondary datacenter.
DR is an optional service that can be included as per customer's requirements</td></tr>
<tr><td>SuccessFactors</td><td>We maintain an N+1 approach for all equipment in the hosted cloud environment, so that there is never a single point of failure. All customer database backups are encrypted and streamed in a secure manner from the customer's "primary" data center to their "alternate" data center, allowing for a timely restoration of service in the event of disaster.
Based on the terms of the agreement, we will designate one of the data centers as the customer's "primary" data center, with an additional data center designated as the "alternate" for data redundancy and disaster recovery purposes.</td></tr>
<tr><td>VMware</td><td colspan="2">VMware IaaS Services
The following table provides common inherent disaster recovery risks and potential mitigation strategies.
<table>
<tr><th>RISK</th><th>Unmitigated Probability</th><th>Mitigation</th><th>Mitigated Probability</th></tr>
<tr><td>Participating agency's lack of a disaster recovery plan leads to</td><td>High Risk</td><td>Participating Entities are encouraged to develop a disaster recovery plan to mitigate against service</td><td>No Risk</td></tr>
</table>
</td></tr>
</table>

	service outage or data loss in the event of a disaster.		outage or data loss. In parallel, entities are encouraged to leverage vCloud Air data protection, vCloud Air Disaster Recovery, and other high availability services while a formal plan is written	
	Participating entity chooses inappropriate data center location leading to service degradation or outage.	High Risk	Participating entities are encouraged to choose datacenter(s) that is geographically proximate to their end users to maximize performance. In addition, location of disaster recovery data center should be geographically separated from primary data center.	Low Risk
	Participating entity fails to budget for and acquire appropriate DR technology leading to inability to recover from disasters.	High Risk	Participating entities are encouraged to include DR capabilities in their costs estimates for cloud deployments to ensure budget is available to acquire those services.	No Risk
	Participating entity fails to ensure cloud service SLAs (e.g. RPO & RTO objectives) meet their mission requirements leading to inadequate service recovery times and data loss.	High Risk	Participating entities are encouraged to review SLAs for each cloud service that they are interested in acquiring to ensure that they meet mission requirements. Care should also be taken to ensure service SLAs do not significantly exceed mission requirements to avoid unnecessary cost.	No Risk
	VMWare AirWatch			

	Providing a secure and stable product that mitigates vulnerabilities, reduces risk and quickly responds to the evolving threat landscape is considered a top priority. Following the guidelines established in NIST SP 800-30, regular risk and vulnerability assessments are performed against the production environment to identify, assess and remediate emerging threats. When potential vulnerabilities are discovered, we follow a documented procedure to prioritize and deploy necessary patches. •Vulnerabilities and threat-sources are identified by conducting interviews with various members of the Cloud Operations community and mapping data to the AirWatch business landscape. •We can provide additional information as conversations progress.
FireEye	Varies by service and customer deployment. Will be defined during engagement setup.
VirtueStream	Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate any known risks. To further mitigate against the unknown, Core microVM's are designed for mission-critical workloads and include reserved compute capacity in a secondary datacenter and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

CA	APM	AWS datacenters provide redundancy and failover within a single AWS EC2 zone (i.e., a single geographic location). Professional Services would need to be engaged to provide multi-geo DR
	MAA	MAA service is currently available from one data center only.
	CA Agile	We run a hot/warm data center configuration and have the ability to quickly failover if required. Our data centers are ~1300 miles apart to ensure redundancy. We perform full system planned switch over testing at a minimum semi-annually.
	ASM	ASM core services run in one primary data center, and can fail over to the DR site if there is a catastrophic failure.
AODocs	As described elsewhere in this response, AODocs is built on Google Cloud Platform (AppEngine) and Altirnao does not manage this infrastructure.	
Virtru	We operate our infrastructure in multiple Availability Zones, and any given data center failure would not result in data loss.	
Salesforce	Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. Our service is collocated in dedicated spaces at toptier data centers. Salesforce's hardware is located inside of secure server rooms designated to Salesforce and separated by concrete walls from other data center tenants. Individual racks inside of the data center are secured with a lock. Specific racks are allocated for hardware supporting the Salesforce Government Cloud. Access to the racks supporting the Salesforce Government Cloud hardware is restricted to Qualified U.S. Citizens as described in the section above.	
ServiceNow	ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region.	

	ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways: •In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center. •Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability. This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized. See the "ServiceNow Security, Operations, and Compliance White Paper" included with this response for more information.
Docusign	Each component of our trusted platform - Hardware & Infrastructure, Systems & Operations, Applications & Access, and Transmission & Storage - undergoes tremendous security scrutiny. HARDWARE & INFRASTRUCTURE Three geo-dispersed, SSAE 16 audited datacenters Near real-time secure data replication and encrypted archival 365x24x7 on-site security Annual Business Continuity Planning (BCP) & Disaster Recovery (DR) testing Third-party penetration testing SYSTEMS & OPERATIONS Physically and logically separate networks Two-factor, encrypted VPN access Professional, commercial grade firewalls and border routers Distributed Denial of Service (DDoS) mitigation Active monitoring and alerting APPLICATIONS & ACCESS Formal code reviews and vulnerability mitigation by third parties Application level Advanced Encryption Standard (AES) 256 bit encryption Key Management & Encryption Program Enterprise-class malware protection Digital audit trail Multiple authentication mechanisms TRANSMISSION & STORAGE Secure, private SSL 256 bit viewing session Anti-tampering controls Signature verification of signing events Unalterable, systematic capture of signing data Digital certificate technology Customer configurable data retention program

QTS	QTS cloud utilizes alternate telecommunications services from both TW Telecom and NTT America that reduces the likelihood of experiencing a single point of failure. QTS's failover facilities in RIC1 and ATL1 are a carrier-class and carrier-neutral datacenter with multiple Internet Service Providers. QTS-FC can establish connectivity with another service provider with 24 hours in the event of an unrecoverable catastrophic connectivity failure of QTS-FC's primary/secondary provider.	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes. Disaster recovery options are included for all Ariba Cloud Services. In the event of a fail-over to the disaster recovery site, no customer changes are required as all URLs that customers use to reach the applications will continue to work. Ariba will notify customers via their email addresses in the event of unplanned downtime. Internally, Ariba uses a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster: Local Ariba staff maintains the hardware remotely. Ariba maintains the application software. Processes are in place to keep database and fileservers in sync between primary and backup data centers. The failover process of all parts of the infrastructure is automated. In the event of a catastrophe, Ariba will declare the primary data center "down" and locally the script will be run to switchover and start the applications at the remote data center. Ariba tests power outage backup scenarios and the Disaster Recovery Plan on a periodic basis to ensure it is up-to-date, successful, and effective.
	Fieldglass	We host and manage the Fieldglass system within secure Internet data centers provided by CenturyLink in Elk Grove, IL, and our disaster recovery center provided by Equinix in San Jose, CA. Both are managed by Server Central which is a Tier 4 hosting provider and a Tier 1 data provider (see the note below). All systems are ""mission-critical loads"" supported by IDC Redundant Power Management System (UPS, generators etc.). Note: Data centers can be classified by tiers, with Tier 1 being the most basic and inexpensive, and Tier 4 being the most robust and costly. According to definitions from the Uptime Institute and the latest draft of TIA/EIA-942 (Telecommunications Infrastructure Standard for Data Centers), a Tier 1 data center is not required to have redundant power and cooling infrastructures. It needs only a lock for security and can tolerate up to 28.8 hours of downtime per year. In contrast, a Tier 4 data center must have redundant systems for power and cooling, with multiple distribution paths that are active and fault tolerant. Furthermore, access should be controlled with biometric readers and single-person entryways, gaseous fire suppression is required, the cabling infrastructure should have a redundant backbone, and the facility can permit no more than 0.4 hours of downtime per year. Tier 1 or 2 is usually sufficient for enterprise data centers that primarily serve users within a corporation. Financial data centers are typically Tier 3 or 4 because they are critical to our economic stability and, therefore, must meet

		higher standards set by our government. Public data centers that provide disaster recovery/backup services are also built to higher standards.
	Hanna	Infrastructure setup: * Standby SAP HEC systems at DR failover site will be shutdown / not useable during regular operations. * WAN connectivity & special requirements (e.g. acceleration services) fall into the responsibil-ity of the customer. * Customer must have independent network connections to both DR sites. * All DR-relevant systems are going to be installed according to the Adaptive Computing (AC) principle (virtual hostnames + virtual IP addresses HSR will be used to replicate data from Primary to DR site for HANA solutions, similarly Sybase Replication Server (SRS) will be used to replicate data from Primary to DR site for ASE based solutions. For more information, please refer to attached Business Continuity document
	SuccessFactors	Our infrastructure architecture is designed with high availability in mind, and engineered for resiliency. All major components are redundant, including power, HVAC, fire suppression, and the physical components of our network. Production data centers have strict access controls, and are continuously staffed and monitored to help prevent acts of sabotage or vandalism. All production data centers are ANSI/EIA/TIA-942Tier III/IV facilities, and are ISO 27001 certified. Production data centers are also geographically dispersed to help prevent a single event from affecting more than one data center. In the event a production data center has an outage we failover to an alternate data center in the same geographic region to minimize impact to customers. Our Cloud Operations teams are also geographically dispersed, working in offices in the US, Europe, South America, and India. Should an office be impacted by an environmental event or pandemic, other offices can continue operations. Aspects of the plan are described in the SOC reports, Disaster Recovery Plan ("DRP") and Business Continuity Plan ("BCP") solutions are dependent on several factors. The customer may be responsible for parts of the recovery/continuity activities
VMware	VMware IaaS Services VMware offers several technologies to provide redundancy, failover capability and the ability to run large scale applications independently in case one data center is lost. vCloud Air is built upon infrastructure that is architected for High Availability leveraging proven vSphere High Availability (HA), vSphere vMotion, and VMware Distributed Resource Scheduler (DRS). These technologies allow participating entities to migrate live workloads and/or automatically restart VMs in the event of host maintenance or unexpected issues. These technologies also maintain a consistently high level of performance for all tenants. VMWare vSphere vMotion enables migration of live VMs to transfer your workloads during maintenance, without downtime. Unlike other cloud providers, VMWare ensures that tenants are not impacted by standard maintenance. VMware performs vMotion migrations for maintenance behind the scenes for its tenants in vCloud Air during maintenance windows without disrupting tenant applications. vMotion is also used to seamlessly migrate VMs from an on-premises environment to vCloud Air and back. Today, vCloud Air is one of only a few major cloud vendors that uses live migration to do maintenance. This capability will enable NASPO participating entities to perform live migrations to move thier applications to and from the cloud for maintenance and other purposes. This	

	technology inherently prevents the lock-in experienced when migrating to cloud services offered by others. VMware Dynamic Resource Scheduler continuously monitors CPU and memory utilization across a cluster of vSphere hosts, allocating resources among VMs and rebalancing performance during high-volume peak times. This is performed 24x7 within the VMware vCloud Air environment. VMware vSphere High Availability delivers the availability required by most applications running in VMs, independent of the operating system and application running in it. Whether participating entities leverage Microsoft Windows or Linux; off-the-shelf or custom developed application; single VMs or many, HA provides uniform, failover protection against hardware and operating system outages within vCloud Air. HA can: • Monitor VMware vSphere hosts and VMs to detect hardware and guest operating system failures. • Restart VMs on other vSphere hosts in the cluster without manual intervention when a server outage is detected. • Reduce application downtime by automatically restarting VMs upon detection of an operating system failure. Other cloud providers require you to build availability in to your application. In the best case scenario, this is as simple as including a load balancer in front of multiple VMs in the same tier to achieve basic high availability. However, often the technologies of other cloud service providers requires a complete redesign of the hosted application, and often network devices such as load balancers are offered at an additional cost, unlike vCloud Air. vCloud Air was built to run hosted applications as-is, providing availability down to a single VM instance, and balancing resources across multiple tenant needs with DRS. Unlike other clouds, with vCloud Air and vCGS, participating entities are not required to rebuild thier application to get the flexibility and agility that cloud can provide. Of course, vCloud Air customers usually do not just stop at moving applications to vCloud Air. Once in the cloud they start to explore features like our Advanced Networking Services and using APIs, automation, and CI/CD tools to deliver services faster. And, where it makes sense, customers do look at application redesigns as well, but with vCloud Air it is not because they must redesign to ensure the application is always available. VMWare AirWatch AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.
FireEye	Varies by service and customer deployment. Will be defined during engagement setup.
VirtueStream	Virtustream's U.S. based data centers are located in Washington, DC, Las Vegas, and San Francisco. All data centers meet the highest industry standard in terms of operational protocol and have redundancy built into all layers of the physical infrastructure. Core microVM's, which are used for mission-critical workloads, provide reserved compute capacity and automatic storage replication so that these systems can be failed over to a secondary data center and have access to the compute capacity required in the event of a catastrophic outage at the primary data center.

8.16 Solution Administration

8.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts.

CA	APM	Customer has full control over all user accounts

	MAA	CA MAA provides user management self-service to customers to manage their own accounts and create accounts for other users.
	CA Agile	The customer is responsible for managing the lifecycle of all user accounts.
	ASM	The Purchasing Entity can manage their account and create sub-accounts within ASM.
Google	Comply	
AODocs	Comply	
Virtru	Virtru does not have an identity system. We federate authentication to Oauth and Email loop verification.	
Salesforce	Identity Management Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application. In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce. Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce. Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product. User Accounts All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security.	
ServiceNow	Customers manage their own instances, including assigning users, defining user roles and profiles, and administrating the system. ServiceNow does not have access to the Customer's instances. The ServiceNow wiki has all ServiceNow documentation available.	

Docusign	Yes, DocuSign allows the purchasing entity to mange identities and user accounts. DocuSign for Enterprise is customizable to meet the administrative needs of the largest organizations. Full administration rights give you total control over document custody and retention policies, how signers sign or adopt signatures, user authentication and more. The branding tools ensure recipients can easily identify documents from your organization.
QTS	24x7x365 Operations Staff - Let QTS provide the expertise and experienced staff to monitor and manage your data center facility. Never again worry about staff turnover or whether your technologists are current with data center best practices.
SAP	Hanna Yes
VMware	VMware IaaS Services VMware management infrastructure requires 2-factor authentication and multiple layers of access control. vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer. control. vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer. VMWare AirWatch The Purchasing entity has the ability to fully manage identity and user accounts for administrators and end users through the web console. Customers can optionally integrate with AD/LDAP to inherit your existing structure and policies.
FireEye	User identity and account settings are controlled within the administration sections of the FireEye cloud solutions.
VirtueStream	Virtustream can provide solution for managed solution for Active Directory or LDAP. As standard, we provide support for managing the VM itself and all OS support. However, our typical use case is, customer manages the users and related activities, as Virtustream might not be aware of internal HR elements of User Management.

8.16.2 Ability to provide anti-virus protection, for data stores.

CA	APM	AWS provides protection/virus scanning for data at rest
	MAA	Logical security is provided by ClamAV Antivirus.
	CA Agile	We have ClamAV installed on all Linux hosts and TrendMicro for Windows hosts.
	ASM	Logical security is provided by ClamAV Antivirus.
Google	Comply	
AODocs	N/A	
Virtru	AlienVault IDS is used to perform virus and vulnerability scans.	
Salesforce	Salesforce runs antivirus software on the production systems that store, transmit or process customer information. The Anti-virus scans host filesystems (not customer data). The antivirus software checks for virus definition updates daily. Other controls are also used to address malware such as hardening the Operating System of our servers, firewall configuration to ensure only required ports are open and all others denied, and use of intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real time through a security monitoring system. The application only accepts http and https traffic, but Salesforce does not restrict the file types users can upload. Salesforce does not modify or clean any customer data; the system stores the information provided in an encoded format within the database. It is recommended that customers run updated antivirus and antimalware solutions to help mitigate these threats. The production system receives inbound mail as part of the workflow functionality, but this does not pose any threat to our network, application, or users. No code in the email can be executed or transferred,	

	eliminating the malicious software risk. Email sent from the Salesforce system is not currently scanned for viruses.
ServiceNow	If Customers want to schedule an antivirus software scan on certain computers after a pre-defined number of days, Customer would define a model-based plan with a duration-based maintenance schedule. This would do the scan automatically to those models defined in the Planned Maintenance area.
Docusign	Yes, DocuSign maintains enterprise-class malware protection.
QTS	Yes - 24x7x365, dependable and detailed support
SAP	Hanna Yes
VMware	VMware IaaS Services Anti-virus software is installed on all development, domain and production hardware devices owned and operated by VMware, which hold company data, passwords, or keys. These devices maintain the most recent version of the anti-virus software signature file. VMWare AirWatch AirWatch has installed a best-in-class, continuously-updated anti-virus suite on servers in the SaaS environment
FireEye	FireEye employs a multi-layered, continuously monitored and engaged set of active defenses to provide anti-virus protection for customer data stores that both meet and exceed traditional approaches. FireEye, and our customers, not only are prepared to reactively withstand attacks from known virus vectors, but since FireEye and our MVX technology is literally, continuously, and securely detonating viruses and other advanced malware on the way to our customer's data stores, FireEye proactively defends from zero day and other emergent attacks as they happen.
VirtueStream	Virtustream offers Anti-Virus protection based on per virtual machine, per month charge.

8.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

Carahsoft will work with each Participating Entity to develop a cost effective plan to assist in the migration and implementation of their data into the new service that has been selected.

8.16.4 Ability to administer the solution in a distributed manner to different participating entities.

Carahsoft will view each Participating Entity as a separate customer and privileges can be assigned for control access even within the individual services.

8.16.5 Ability to apply a participating entity's defined administration polices in managing a solution.

Each Participating Entity will have the ability to work with Carahsoft and the Service Provider to identify defined administration policies to mangage the solution.

8.17 Hosting and Provisioning

8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

CA	APM	CA SaaS Ops has a well defined Service Introduction and update process, including review boards, staged rollouts and followups to ensure service integrity. Our cloud provisioning stack is tied to AWS EC2 services, and includes S3 and RDS for storage; RHEL instances for the applications; route 53 DNS services; cloudfront for monitoring; and ELB for load balancing

	MAA	Automation tools are used to install and configure MAA software on CA infrastructure. SOP documents are used by CA internally.
	CA Agile	All new systems should be provisions according to our baseline standards and we use configuration management tools to ensure all systems are created with the same standards.
	ASM	Automation tools are used to install and configure ASM software on CA infrastructure. SOP documents are used by CA internally.
Google	Google has administrative document and Google Deployment Guides accessible on the web.	
AODocs	This is not applicable to Google.	
Virtru	Ubuntu AMIs provisioned using terraform and configured by Ansible	
Salesforce	Cloud Hosting and Provisioning Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Government Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Salesforce provides market leading PaaS and SaaS solutions and is a multitenant cloud-based subscription service. Multi-tenant cloud solutions provide a single, shared infrastructure, one code base, one platform that is all centrally managed, with platform-based API to support all integration traffic, and multiple release upgrades included as part of the subscription service. Multi-tenancy and the Cloud Computing model remove unneeded tasks from the process of delivering, managing, and integrating software. Salesforce customers will not need to maintain any hardware or software. Without multiple versions to support, integrations don't break during updates; they are simply updated automatically. As a result, both the initial integration and its continued maintenance are simplified. More resources can be focused on creating a better product, with a faster cycle of innovation, instead of having to manage the complexity of many different versions to support a vast installed base. Salesforce's position as an online service enables us to roll out all levels of improvement, from patch releases to major upgrades, that are largely transparent to the end users. When a bug is fixed and tested, it is rolled out to the application as part of regular maintenance; the nature of the service prevents special patches and code branches for individual customers, so all fixes can potentially benefit all customers. The Salesforce Services is delivered using a world-class data center infrastructure. Each customer's org is hosted from a primary and secondary production data center, with near real-time replication occurring between the two sites. Salesforce is a pure multi-tenant web application. No software or infrastructure is required by the customer other than a computer, browser and internet connection or a mobile device. User Administration and ProvisioningUser provisioning and management is performed by the customer through the Salesforce Administrative Setup environment. Users, their profiles, permissions and passwords may be managed, edited, activated and deactivated as needed by those with appropriate permissions. An administrator with appropriate privileges can manage session timeout, password policies, IP range login restrictions, delegated authentication/SSO, and requirements as part of this process. On first time login or password reset request, users are required to change their passwords to gain access.	
ServiceNow	ServiceNow includes all documentation on the wiki at wiki.servicenow.com.	
Docusign	DocuSign hosts customer accounts in its own data centers managed by DocuSign. Upon a new contract executed with a customer, DocuSign provisions a customer account based on the	

	contract terms. A designated point of contact becomes the default primary administrator who then adds additional users and other admin tasks. DocuSign's cloud stack is defined in architecture documents available under separate confidential disclosure.	
QTS		
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	Fieldglass maintains its own platforms and follows a mature change control process for introducing new systems to the hosted environments.
	Hanna	The Managed Service includes the following: • Infrastructure operations management: monitoring, patching, software updates & maintenance up to the OS Layer • OS management: monitoring, patching, updates, and maintenance of the specific OS • Network and system administration • HANA database platform operations includes: space management revision management , security management , hardware configuration management, backup & recovery, change management coordination • Health check services, proactive monitoring, capacity management • SAP Technical Application Basis Operations (incl. SAP Basis) • Monitoring • Troubleshooting – Incident Management Level 2 and 3 • Patch Management • Housekeeping • Backup/Recovery
	SuccessFactors	We offer a cloud based solution. Our application is standardized on the J2EE technology stack with the majority of our software written in industry-standard software programming languages, such as Java. We also make extensive use of Web 2.0 technologies, such as AJAX and Flash, for improved usability and performance and to deliver a rich and highly interactive experience. Our hardware consists primarily of industry standard web servers, application servers, database servers and storage and networking equipment. Customers share the network security infrastructure, web servers, application servers and database instance, and each customer has their own set of database tables that are logically partitioned in the database containing its own unique database schema. Each company instance can be completely exported out of the database without affecting any other customer. The application utilizes the JAVA and J2EE industry standards. Integration is supported through .CSV, XML and web services standards. The application is portable to any platform and is deployed on Apache (Solaris) Web Servers, JBOSS Application Servers, and Veritas High Availability Cluster Servers, and utilizes Cisco Networking.
VMware	VMware IaaS Services An interface that allows users to select from a catalog of pre built OS images and allows them to provision on the fly.	

	VMWare AirWatch AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers. Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.

8.17.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

CA	APM	New servers are predefined by the CA SaaS Ops toolchain, and automated using AWS tooling to be able to bring up/down servers on demand
	MAA	Same as above.
	CA Agile	We utilize configuration management tools to ensure consistent configuration across our servers.
	ASM	Same as above.
Google	1. This is not applicable to Google. Capacity planning and server deployment is fully managed by Google. 2. This is not applicable. With the Google IaaS solutions all server images are provided by Google. 3. With respect to the SaaS offfering, Google Apps, if customers have not selected the Google Apps Unlimited option which offers unlimited storage, they have options to upgrade. With respect to the PaaS/IaaS offering, Google Cloud Platform, storage space is allocated dynamically based on actual usage demand. 4. SaaS, Google Apps includes numerous administrative tools to monitor end user and administrator activites."	
AODocs	This is not applicable.	
Virtru	AMIs provisioned using terraform and configured by Ansible to include all configuration parameters	
Salesforce	This is not applicable. These services while applicable to IaaS are not applicable to PaaS/SaaS where all of the infrastructure is managed by Salesforce as the Cloud Service Provider. These services are included and managed as part of the Salesforce subscription service and not directly exposed to the customer. The multitenant architecture and secure logical controls address separation of customer data. There are no dedicated servers used for individual customers. The Salesforce Services infrastructure is divided into a modular architecture based on "Instance". Each Instance is capable of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer's org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers. An instance consists of a database instance run on clustered database servers and physical storage subsystems. Each server has been allocated a different volume group so it can fail over to its backup server within the instance independently of the others. As scalability needs dictate,	

	additional database instances can be brought online (the application already provides for this). For additional server capacity, one or more databases could be moved onto its own database server.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
SAP	Ariba	Operating systems when installed through default means and with default settings are typically not secure and often include applications and services not required. Ariba has standardized operating systems' installations based on best practices. Ariba servers are configured with just the applications and services required to run the server as designed. Services not required are disabled and binary files not required for operation are removed, which reduces the total number of vulnerabilities a system may have. Ariba standardized installation process also ensures that all servers of the same type are configured exactly the same, utilizing a process that initiates an upgrade to system binaries across all systems. Based on the system type, the configuration will remain the same. If one server type needs to receive a patch for a vulnerable binary file, that patch is pushed to all systems of that particular server type. If that binary exists on all systems, it is patched across all systems. Patches are then included in the build process as well so that future systems built are in compliance with security standards. Ariba uses this configuration process to 'harden' the operating system prior to implementing additional controls as detailed below.
	Fieldglass	Fieldglass uses group policy to ensure the configuration of all servers match our security requirements.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
	SuccessFactors	We apply hardening in line with ISO 27k standards and audit key areas in the SOC 2 Type 2 report. Audit reports are available to customers and prospects upon completion of an NDA.
VMware	VMware IaaS Services vCloud Hybrid Service provides an interface that allows users to select from a catalog of pre-built OS images and allows them to provision on the fly. vRealize Automation is the next level for provisioning, delivering, and managing IT services on VMware vSphere infrastructure as well as VMware vCloud Air all with a unified management experience. It provides governance and blueprints to deliver services from on premise into vCloud Air. Customers can integrate vCloud Air with vRealize Automation. In this setup, users access vCloud Air primarily through the vRealize Automation service catalog which handles authentication to the service itself. vRealize Automation supports VMWare AirWatch AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	
VirtueStream	Virtustream offers on-demand self-service portal where State of Utah can deploy new servers as stand-alone or part of a server farm.	

2. Creating and storing server images for future multiple deployments

CA	APM	Servers are brought up on demand

	MAA	Same as above.
	CA Agile	We utilize configuration management tools to ensure consistent configuration across our servers.
	ASM	Same as above.
Virtru	Provisioning system automatically persists all past AMIs for ability to roll-back	
Salesforce	This is not applicable. These services while applicable to IaaS are not applicable to PaaS/SaaS where all of the infrastructure is managed by Salesforce as the Cloud Service Provider. These services are included and managed as part of the Salesforce subscription service and not directly exposed to the customer.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
SAP	Ariba	Ariba has standard 'realms' which are default versions of the various configurations the Ariba on-demand products can be setup for each customer with one test and one production instance. Ariba maintains all hardware, software, realms and entitlements taking the burden off our customers and suppliers whilst providing a platform to configure to each company's needs and business processes
	Fieldglass	Fieldglass uses virtual servers within our hosted environments uses the hardening configurations to maintain the right level of security.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
VMware	VMware IaaS Services We also allow for template and gold master images to be stored on-premise and deployed to the cloud as well as storage of templates and master images in vCloud Director catalogs in in vCloud Air VMWare AirWatch Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	
VirtueStream	Virtustream offers server images, templates, or other methods (OVF and blueprints) for multiple deployments as part of standard solution.	

3. Securing additional storage space

CA	APM	AWS EC2 storage is elastic, and can be expanded on demand
	MAA	Virtual storage can be added when needed.
	CA Agile	We have redundant systems for all critical infrastructure and have the ability to add additional storage if deemed necessary.
	ASM	Additional storage is added manually.
AODocs	AODocs storage is based on Google Apps Drive storage and with respect to the SaaS offfering, Google Apps, if customers have not selected the Google Apps Unlimited option which offers unlimited storage, they have options to upgrade.	
Virtru	New hardware added at Cloudant	
Salesforce	Salesforce provides extensive storage capabilities. Storage is divided into two categories: file storage and data storage. File storage includes files in attachments, the Documents tab, the Files tab, the File field, Salesforce CRM Content, Chatter (including user photos), and Site.com assets. Data storage includes the following entities/records stored within the Salesforce application: Accounts, Article types, Article type translations, Campaigns, Campaign Members, Cases, Case	

	Teams, Contacts, Contracts, Custom objects, Email messages, Events, Forecast items, Google docs, Ideas, Leads, Notes, Opportunities, Opportunity Splits, Orders, Quotes, Quote Template Rich Text Data, Solutions, Tags: Tag applications, Tags: Unique tags, and Tasks. For file storage, Unlimited Edition is allocated a per-user limit multiplied by the number of users in the organization plus an additional per-organization allocation. For example, an Unlimited Edition organization with 600 users receives 1,211 GB of file storage, or 2 GB per user multiplied by 600 users plus an additional 11 GB. For data storage, Unlimited Edition is allocated either 1 GB or a per-user limit, whichever is greater. For example, an Unlimited Edition organization with 10 users receives 1 GB because 10 users multiplied by 20 MB per user is 200 MB, which is less than the 1 GB minimum. Additional storage can be purchased, or files can be exported and archived outside of Salesforce, thus freeing up file storage space.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
QTS	Services that scale to meet your web and IT infrastructure needs - QTS offers space options from single cabinets to multi-rack cages to private suites. Coupled with configurable primary and redundant power options to run your infrastructure, QTS Colocation services can be scaled to support your near term growth requirements and future expansion.	
SAP	Ariba	We carefully monitor all network interfaces. Internally we are well below capacity on our most congested interconnects. To the internet we use Border Gateway Protocol to peer with redundant Internet Service Provider's and manage the bandwidth accordingly.
	Fieldglass	As a software-as-a-service (SaaS), Fieldglass automatically and transparently handles the scaling and redundancy for customers based on SLAs governing performance and availability. Fieldglass monitors application servers, database servers, bandwidth, and infrastructure for average and maximum utilization with Orion. Current utilization averages approximately 20 percent across all components with a goal of scaling the component vertically or horizontally (depending on the specific component) upon reaching a 60 percent threshold). All systems are scalable either horizontally or vertically to handle capacity requirements. This includes but is not limited to web servers, database servers, and storage.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
VMware	VMware IaaS Services Additional storage can be purchased and provisioned in 48 hours. VMWare AirWatch Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

CA	APM	all SaaS based instances are monitored by CA SaaS Ops. With Hybrid deployments, customers can manage the on premise components of the deployment using their own tooling or CA products
	MAA	MAA is monitored internally as well as externally using multiple tools recognized within industry.
	CA Agile	Access to monitoring tools is provisions according to the principle of least priviledge and is only granted based upon business need.
	ASM	ASM uses Nimsoft Monitor, third-party open source monitoring tools, and ASM itself to monitor the health of ASM internal services and servers.
AODocs	AODocs includes numerous administrative tools to monitor end user and administrator activites.	
Virtru	Dtrace, CloudWatch, CloudTrail, Logstache, ElasticSearch, Kibana, DataDog	
Salesforce	Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find: ● Live and historical data on system performance ● Up-to-the minute information on planned maintenance ● Phishing, malicious software, and social engineering threats ● Best security practices for your organization ● Information on how we safeguard your data System Overview In addition to our Trust site (http://trust.salesforce.com/trust/status), you will also have access to a System Overview, which will help Salesforce customers monitor performance and usage of their own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used Licenses API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages Portal The above list is of all the possible metrics that Salesforce customers may have in their system overview.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
QTS	Alert Logic's Threat Manager Intrusion Detection System (IDS) and Vulnerability Scanning functionality are designed to monitor, detect, report and alert on adverse security issues on behalf of our customers. Within this process there are a number of both automated and manual processes which are supported by our SIEM software ('The Expert System') as well as our Network Security Analysts in our Security Operations Center (SOC). Threat Manager is the Alert Logic IDS and VA scan product. It includes the physical or virtual appliances and software tools used to analyze the customer's infrastructure and monitor that infrastructure for attacks. ActiveWatch is the managed aspect of Threat Manager, providing 24 x 7 monitoring and incident response operations from the Alert Logic SOC. Threat Manager's Expert System identifies valid security events and suppresses false positives through a patented multifactor correlation process. Every security event monitored by its global network of threat sensors is analyzed in real time. When the Expert System determines that a set of events comprise a valid security threat, an incident is created and escalated according to severity via email or through an Alert Logic Network Security Analyst. This approach dramatically	

	reduces false positives and keeps analysts and customers focused on real, actionable incidents. In addition, Alert Logic's security research team continuously monitors threat data and tunes the Expert System to respond to the most current threats.	
SAP	Ariba	Within our solution, specific logging takes place that is viewable by the customer administrator or their designee. Audit logs produced through use of the solution are considered customer data and are maintained within the customer's instance of the database. These logs are retained so long as the customer has an active contract with us. As a user control consideration, customers are responsible for monitoring the proper entry of data to the solution and reviewing reports generated by the system.
	Fieldglass	Fieldglass has a comprehensive set of performance monitoring tools in place. Some tools are built in the application and some are external. The Fieldglass application captures every page hit and the time it takes to respond. It captures the server response time and the client rendering time separately. The average page times are available to be seen by privileged users through the application. The user can drill down to the hour or minute or a single request for analysis. The information can be displayed by time range for all users, by company, or even for an individual user. Orion Network Monitoring watches more than 1,000 different points of interest on the production infrastructure. These monitors include, but are not limited to, the following: CPU, Memory, I/O, Capacity and Synthetic Transactions. These monitors along with our custom application performance monitors are used to produce and comply with customer SLA requirements. Fieldglass also uses Splunk Enterprise Security for event/audit log collection and correlation. Events and logs are retained online for 90 days and offline for two years. Alerts are generated and reviewed as they occur.
	Hanna	SAP HEC uses Solution Manager for monitoring the infrastructure end to end.
	Hybris	SAP Hybris offers continuous 24/7 systems monitoring in-place, which automatically notifies you, SAP Hybris support and optionally your designated implementation partner in the event of any monitored system problem. Tools used for monitoring include HP Sitescope and Nagios. This service ensures quick response times to emergency problems. Standard monitors are in place for basic site availability. Customer can utilize additional 3rd party monitoring services should it wish to add additional monitoring. Upon request, monthly or quarterly reviews are offered to review performance over the period. When a system problem occurs, in addition to monitor alerts sent to the customer, SAP Hybris support may send emails to a designated customer notification email address to provide status, updates or further detailed information. In addition, a support ticket would be created which would include such information.
	SuccessFactors	The application logs the following for every transaction: Event/transaction Time, Transaction ID, Event/transaction Type, Event/transaction Status (Result of the event; if failure, includes reason), Object Attributes (Describes the object affected by the event), Originator User ID (ID of the user who initiated the event or action), Subject ID, Process User ID, Account Number, Transaction Specific Elements. The application audits changes to the major components. Examples of this are goal auditing and document auditing. The audit trail includes who made the change, the date of the change and the ability to see the data as it existed at

		that point in time. The data in the audit log can be viewed with appropriate permissions. We also provide an optional Audit Framework for additional audit logging capabilities. All audit logs within the application are accessible only by customers. Therefore, the review of application audit logs as well as retention periods for the application audit logs are the customer's responsibility, and can be determined as per requirements
VMware	VMware IaaS Services The vCloud Hybrid Service infrastructure, including the top layer management stack, the customer management stack and the computing/storage/network hardware are monitored for availability, capacity and performance. Customers are responsible for monitoring their own VMs (OS, apps). Customers can use on premise monitoring tools to manage and monitor their applications and OSes over VPN and direct connect. VMWare AirWatch The AirWatch Cloud Operations team monitors the SaaS environment. AirWatch follows the Fault, Configuration, Accounting, Performance, and Security (FCAPS) model to monitor the SaaS environment. •We have configured the system to notify support personnel of any issues with key performance items •Because the solution is built on industry-standard ASP.NET architecture, it integrates into existing management and monitoring tools. Administrators can configure log data storage to destinations such as Windows Event Viewer, SNMP traps, syslog, SMTP email alerts, etc. The solution also integrates directly with Microsoft SCCM. The communication layer includes a complete infrastructure for API integration to third parties as well as a rich set of existing APIs, web services, single sign on and authentication protocols. Integrate with security information and event management (SIEM) solutions for enhanced logging of events occurring in the console. Administrators can view events, filter by event type, category and module, and export events. Event logging settings can be configured based on severity levels, with the ability to send specific levels to external system via syslog integration.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	

8.18 Trial and Testing Periods (Pre- and Post- Purchase)

8.18.1 Describe your testing and training periods that your offer for your service offerings.

Training and testing periods will vary based on the Service provider as well as the complexity of the request that is made by the Purchasing Entity. Some of the services can be functional within a few days and some will take a few months for full implementation.

8.18.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Upon Request, Carahsoft will provide access to any of the Cloud Technologies proposed. The precise Access to the technology may be in a limited or "DEMO" fashion. Access will be to an extent that the State may complete any necessary tests or verifications that may be required. Instructions on precisely how each technology will be accessed will be provided upon request. All of the proposed technologies are currently live/ active and support many customers. A specific instance of the requested technology would be stood up within the cloud framework to support this request. As this will be occurring within a production, the creation of the instance is a quick and straight forward process not requiring any sort of extraordinary effort.

8.18.3 Offeror must describe what training and support it provides at no additional cost.

Carahsoft provides the customer with free training for specific deals on a case by case basis. This can include free installation, training, and maintenance for high value customers who purchase Carahsoft's solution through the NASPO contract vehicle. In addition, Carahsoft will provide webinars with basic training on a quarterly basis, made available to any Purchasing Entity who wishes to participate.

8.19 Integration and Customization

8.19.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

The integration into other applications will vary base on the Service Provider, however it is standard practice to allow for open AIs for integration development. For example Connecting Salesforce to an existing enterprise application is a common and frequently performed task. Integration options range from native Web Services support (APIs, outbound workflow, etc.) to import/export utilities to middleware integration via packaged connectors to toolkits for Java, .NET, and other open platforms. Our solution provides the ability to call out to virtually all common APIs, to enable synchronization, push / pull, and mash-ups with external apps/systems. Salesforce itself is based on web-service based APIs that in turn simplify access to Salesforce data from external systems. API-based integration is heavily leveraged by our customers.

8.19.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

The Service Providers customization options are very extensive and highly configurable. For example The Salesforce Platform offers a core set of technologies that not only power the Salesforce SaaS products, but also allows your Agency to build custom apps, connect data from any system, and manage it from anywhere. The Salesforce Platform allows customers to build apps fast with just a few clicks, designed for desktop and mobile devices, all from a single canvas. The Salesforce Platform has been given top ratings by Gartner, Forrester, & Info-Tech Research. To help IT deliver apps faster, the Salesforce Platform offers a simple yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Salesforce Lightning Builder tools allows your Agency to work in alignment with agile development methodologies as IT meet business demands faster. The Platform uses open APIs based on industry standards such as REST and SOAP to make it easy for your Agency to build apps that integrate with legacy systems. For more complex applications, developers can leverage the Apex programming language. Apex is an object-oriented, on-demand language. It is like Java, with similar syntax and notation, and is strongly-typed, compiled on demand, and fully integrated into the Platform. All of the application services come right out of the box, from a powerful workflow engine to API services, integration services, authentication, event log framework, analytics, and collaboration.

8.20 Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Carahsoft offers deep experience in public sector marketing. Our dedicated team plans, promotes and executes more than 2,000 public-sector marketing campaigns and events each year, including contract-specific promotional activities. These include but are not limited to:

- News announcements

- Social media promotion (Twitter, Linked In, Facebook, Carahsoft Community)
- Website content/reciprocal links (Carahsoft website page; content for contract sponsor page)
- Marketing materials (FAQs, contract overviews, solution spec sheets, powerpoint slides)
- Training documents
- Co-branded tradeshow graphics, giveaways, display materials
- Tradeshow participation (national, state and local government and education shows)
- Digital and print ads
- Webinars
- Email campaigns
- Proactive marketing opportunity tar available through:
  - National Coalition for Public Procurement (NCPP) – publicprocurementcoalition.org
  - Institute for Public Procurement (NIGP) – nigp.org
  - National Association of Counties (NACo) – naco.org
  - The United States Conference of Mayors – usmayors.org
  - National League of Cities – nlc.org
  - National Governors Association – nga.org
  - Relevant State Associations

8.21 Related Value-Added Services to Cloud Solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

In addition to Carahsoft's quoting and configuration expertise, we also have a wide range of Service Provider implementation partners that we leverage to work with Purchasing Entities in order to ensure successful adoption and deployment within a Purchasing Entity. We will help to identity needs for initial setup, training and access to the services so that it is all available at the best prices from one source to the Purchasing Entity.

8.22 Supporting Infrastructure

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

The Service Providers that are being proposed operate on their own secure infrastructure. The Purchasing Entities will only need an internet connection to access the services.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

The Service Providers maintain all costs for updating and building new infrastructures.

8.23 Alignment of Cloud Computing Reference Architecture

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

CA	APM	The SaaS portal runs in Amazon Web Services.
	MAA	CA MAA is a SaaS service.
	CA Agile	Only SaaS is being offered via a public cloud

	ASM	As a monitoring service, ASM is considered to be SaaS.
Virtru	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2 . The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.	
Salesforce	Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Government Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Salesforce was the first Cloud Service Provider to attain FedRAMP Authority to Operate for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls. Salesforce does not provide IaaS as a direct service offering to our customers, it is an underlying part of our PaaS and SaaS offerings. Salesforce Government Cloud In May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4. Testing for the ATO was performed by a third party assessment organization (3PAO). The Salesforce Government Cloud information system and authorization boundary, is comprised of the Force.com Platform, Salesforce Services (Sales Cloud, Service Cloud, Chatter), and the backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS). To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS guidance. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18, Guide for Developing Federal Information System Security Plans. The SSP identifies control implementations for the GSS and in-scope customer facing products (Force.com Platform, Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a third party assessment organization (3PAO) in accordance with NIST 800-53A and FedRAMP requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of the Salesforce service and the customer data it stores, transmits and processes. To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring. Continuous monitoring includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and at least annual independent assessment of a selection of security controls by 3PAO. As part of our FedRAMP annual assessment, Salesforce is now aligned with NIST SP 800-53, Rev. 4 controls.	
ServiceNow	ServiceNow's architecture aligns with Software as a Service (SaaS).	

Docusign	DocuSign's DTM® solution is ISO 27001:2013 certified and many of the ISO 27001:2013 controls are mapped to the NIST 800-53 requirements; we can provide additional information upon request.	
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	Fieldglass is offered in a SaaS model. We follow the public cloud model identified by NIST. All customers access the same Fieldglass application version in a multi-tenancy database. The system is hosted in a secure hosting facility. Fieldglass manages everything from the cage in including all servers, devices, wiring, software, and configuration. Fieldglass uses the Cloud Security Alliance framework to measure itself against the recommended controls, in addition to ISO 27001 and SOC 2 controls in the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy.
	Hanna	HEC is a private cloud offering from SAP that provides fully 'managed' Infrastructure as a Service (IaaS) following NIST Cloud Computing Reference Architetcure.
	Hybris	The SAP Hybris Commerce, Cloud Edition is a Private Cloud Managed Service that offers a best practice multichannel commerce platform built on hybris accelerator technology, running in SAP Hybris own datacenters with a pay as you grow subscription model.
	SuccessFactors	Our IT architecture is aligned with ISO 27002. We are Safe Harbor certified and in alignment with BS10012 and ISO 20000 for Service Delivery. We demonstrate an on-going commitment to protecting the confidentiality, integrity and availability ("CIA") of data from internal and external threats, making us a reliable and secure system provider. Our secure multi-tenant Software as a Service (SaaS) platform is designed for availability, security, scalability, and performance. Industry best practices and standards are adopted and incorporated. Our Network also complies with the Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We provide privacy compliant data center facilities not only in the United States but also as a Member State of the European Union (EU) or a state of the European Economic Area (EEA). Currently, such data centers are certified for ISO27001, ISO9001 and PCI-DSS compliance. Our security services provide complete and thorough monitoring of all traffic on the network on a 24x7x365 basis, and include security technology, alert services and incident management support. We are audited twice annually to SSAE16 (US) or ISAE 3402 (international) accounting standards.

<table>
<tr><td>VMware</td><td>See section 8.1.1 for additional details.

Due to FOIA restrictions, we cannot share specific infrastructure details or architecture diagrams at this time. We can provide sample architecture diagrams under NDA to participating entities during task order negotiations as required.

VMWare AirWatch
AirWatch partners with co-located and cloud-hosted Tier III data centers to support of SaaS offering.
Due to FOIA restrictions, we cannot share specific infrastructure details or architecture diagrams at this time. We can provide sample deployments as under NDA to participating entities during task order negotiations as required.</td></tr>
<tr><td>FireEye</td><td>Each of the FireEye cloud solutions are classified as Software as a Service (SaaS) and leverage a private cloud deployment model. With respect to the NIST Cloud Computing Reference Architecture, the following actors are integral to the overall design of the solutions:

<table><tr><th>Actor</th><th>Definition</th></tr><tr><td>Cloud Consumer</td><td>Customer organizations who have purchased FireEye cloud solutions</td></tr><tr><td>Cloud Provider</td><td>FireEye</td></tr><tr><td>Cloud Carrier</td><td>Internet service providers and organizations who have been contracted to host FireEye cloud solutions.</td></tr></table>
A Cloud Broker is not leveraged in the FireEye cloud offerings. FireEye has contracted independent service auditors for evaluating controls relevant to security and confidentiality, however this occurs on an as-needed basis.</td></tr>
<tr><td>VirtueStream</td><td>Virtustream solution is fully NIST compliant for Essential Characteristics, as the Infrastructure as a Service (IaaS) Service Model, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud. To that extent:
1.Virtustream IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP.
2.Virtustream IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, NetBond, etc.) which is growing rapidly as option for connecting cloud resources.
3.Key to Virtustream solution is its proprietary and patented solution of uVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level.
4.Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for State of Utah allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool.
5.The fundamental of Virtustream solution is based on uVM Technology, which is very unique in terms of billing. Virtustream solution takes average consumption of compute resources, and State of Utah would only pay for actual resources based on a monthly average. This is in comparison</td></tr>
</table>

	with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the Virtustream solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, Virtustream can provide consultative and project support based on time and materials. 6.The deployment of Virtustream cloud can be on-premise or private based on purchase of its Cloud Management Platform, Community Cloud based on its IaaS, Public Cloud based on its IaaS and Hybrid cloud based on its ability to provide software and IaaS combined.

CONFIDENTIAL, PROTECTED, OR PROPRIETARY INFORMATION

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

Carahsoft Technology Corporation ("Carahsoft") respectfully requests that section 6.3 Financials of Carahsoft's response be treated as a trade secret under the Utah Uniform Trade Secrets Act, Utah Code § 13-24-2 and submits this justification in accordance with Utah Code 63-G-2-305 demonstrating that its audited financials should be treated as a trade secret under Utah's Uniform Trade Secrets Act. Additionally, Carahsoft is claiming the same confidentiality of the Consensus Assessments Initiative Questionnaire provided in relation to DocuSign and FireEye offerings, as well as the Cloud Controls Matrix for DocuSign.

Carahsoft has marked this attachment as "confidential" in accordance with the RFP instructions by including all confidential data into the Confidential, Protected, or Proprietary Information in our response.

Carahsoft is claiming confidentiality for these specific Consensus Assessments Initiative Questionnaires and Cloud Controls Matrix because releasing these documents would cause irreparable damage and would create the potential for cyber security breach. While portions of this information are in the public domain, the information contained within is not represented or assimilated this way in any other format.

Carahsoft's Audited Financial Data satisfies the three-part test of the Utah Uniform Trade Secrets Act as set forth below and should therefore be treated as confidential and by the Utah Division of Purchasing and should not subject to public disclosure as provided in Utah Code § 63G-2-305.

1. *Carahsoft's Audited Financial Data is a "compilation" within the meaning of Utah Code § 13-24-2(4).*
Carahsoft's Audited Financial Data is a compilation of all of the Company's financial data and results for 2014. While some aspects of this information may be available, the compilation of this information is unique and the result of sustained and distinct effort by the Company's financial staff and its accountants.

2. *As required by Utah Code § 13-24-2(4)(a) Carahsoft derives independent economic value, actual or potential, from its Audited Financial Data not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.*
Carahsoft is a leading distributor of technology products and services to public sector customers such as the State of Utah, and throughout the United States and Canada. Sales in this market are intensely and deliberately competitive, with each sale subject to a structured bidding process in which low price is frequently the deciding factor on which contract award is based. Competition in this market is fierce, with competitors regularly competing with one another for federal, state, county and city business.

Carahsoft's competitors closely monitor this market, and regularly attempt to gain financial and other information about Carahsoft and other competing vendors. Allowing Carahsoft's competitors access to this compilation of financial data by releasing it in response to a public records request will damage Carahsoft's competitive position because it will provide competitors insight into Carahsoft's financial structure, including compensation, overhead costs, rental rates, profit margins and the like. Indeed, allowing insight into compensation may violate individual employees' expectations of privacy. Once competitors have this access and insight, they can use it to undercut Carahsoft in the marketplace, damaging Carahsoft's business with its customers and its suppliers, and inflicting economic hardship upon the Company.

For these reasons, Carahsoft does not itself disclose its Audited Financial Data except when required by law to do so. For example, Carahsoft discloses its financial information in filing its periodic tax returns—disclosure of which is prohibited by applicable state and federal law. In this regard, we note that Carahsoft is a privately owned company. Therefore, Carahsoft does not publicly report its financial results to the United States Securities and Exchange Commission.

3. Carahsoft uses reasonable efforts to maintain the secrecy of its Audited Financial Data.

The third part of the Utah Uniform Trade Secret Act's test for trade secret treatment is whether the information "…is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Utah Code § 13-24-2(4)(b).

Carahsoft satisfies this test because it takes reasonable steps to maintain the secrecy of its financial information. As noted above, Carahsoft is a privately held company and therefore does not report its financial results publically to either its shareholders or the Securities and Exchange Commission. This is in contrast to public companies such as IBM or AT&T who report financial results quarterly as a matter of public record.

Even within Carahsoft's business operations itself, Carahsoft's management strictly limits disclosure of this information to a few carefully selected employees, and then only on a "need to know" basis in connection with their work assignments. Indeed, each Carahsoft employee signs a Confidentiality Agreement agreeing not to disclose this information.

Conclusion

Based on the forgoing, Carahsoft believes it has demonstrated that its Audited Financial Data, Consensus Assessments Initiative Questionnaires, and Cloud Controls Matrix are trade secret as defined in Utah Code § 23-24-2 . It is a compilation the content of which affords Carahsoft a competitive advantage. Carahsoft's competition cannot readily discern it by proper means. Moreover, Carahsoft itself treats this information as a trade secret even within its own business operations.

Should there be a public records request for this information, Carahsoft respectfully requests that the State afford Carahsoft's requested confidential information and documents trade secret protection in accordance with Utah law and deny the request. In the event that the State determines to release the requested confidential data, Carahsoft requests that you notify us promptly so that we may provide further justification for trade secret protection of this confidential data.

CLAIM OF BUSINESS CONFIDENTIALITY

Pursuant to Utah Code Annotated, Subsections 63G-2-305(1) and (2), and in accordance with Section 63G-2-309, Carahsoft Technology Corporation (company name) asserts a claim of business confidentiality to protect the following information submitted as part of this solicitation. Pricing/Cost Proposals may not be classified as confidential or protected and will be considered public information. **An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY".**

☒ Non-public financial statements
☐ Specific employee name and contact information
☐ Specific customer information, client lists, or subscription lists
☒ Other (specify): Consensus Assessments Initiative Questionnaires and Cloud Controls Matrix

This claim is asserted because this information requires protection as it includes:

☒ trade secrets as defined in Utah Code Annotated Section 13-24-2 ("Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy).

☒ commercial information or non-individual financial information obtained from a person if: (a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future; [and] (b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access.

This statement of reasons supporting the claim of business confidentiality applies to the following information in this proposal:

Page	Paragraph	Reason
187-204, Technical Response Template	All	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 1-DocuSign Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 1-FireEye Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 2-DocuSign Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response

Please use additional sheets if needed.

You will be notified if a record claimed to be protected herein under Utah Code Annotated § 63G-2-305(1) or (2) is classified public or if the governmental entity determines that the record

should be released after weighing interests under Utah Code Annotated § 63G-2-201(5)(b) or Utah Code Annotated § 63G-2-401(6). See Utah Code Annotated § 63G-2-309.

Signed: Robert R. Moore, Vice President
On behalf of (company): Carahsoft Technology Corporation
Date: March 10, 2016

(Revision 6/4/2015)

EXCEPTIONS AND/OR ADDITIONS TO THE STANDARD TERMS AND CONDITIONS

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing.

Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations. If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

The point of contact who will be directly involved in terms and conditions negotiations is Jack Dixon – Contract Specialist. He can be reached at – 703.230.7545 / Jack.Dixon@Carahsoft.com.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

Carahsoft takes exception to section 32 – Transition Assistance and request it includes the following.

9.4 RETURN OF CUSTOMER DATA. Carahsoft shall provide Customer Data in its standard database export format, excluding the any Core Technology, to Customer upon Customer's written request and at no additional cost to Customer, provided that Carahsoft receives such request from Customer within forty-five (45) days following the expiration or termination of a provided service. If Carahsoft has not received a request within the foregoing time frame, Carahsoft shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of any provided service.

Carahsoft takes exception to Section 13 – Indemnification. Carahsoft requests that Indemnification from the state to the customer under a certain set of circumstances.

IN SUMMARY

Carahsoft Technology Corporation appreciates the opportunity to offer this solution for the State of Utah's initiative.

The Carahsoft Team has proposed a superior and cost-effective solution that fully complies with the State of Utah's requirements set forth in Solicitation # CH16012. We understand the importance of your project goals, and we are confident you will benefit from this solution and our expertise.

Carahsoft looks forward to the opportunity to speak with you regarding the details of this proposal, as well as the opportunity to work with the State of Utah on this project.

SUPPLEMENTAL INFORMATION

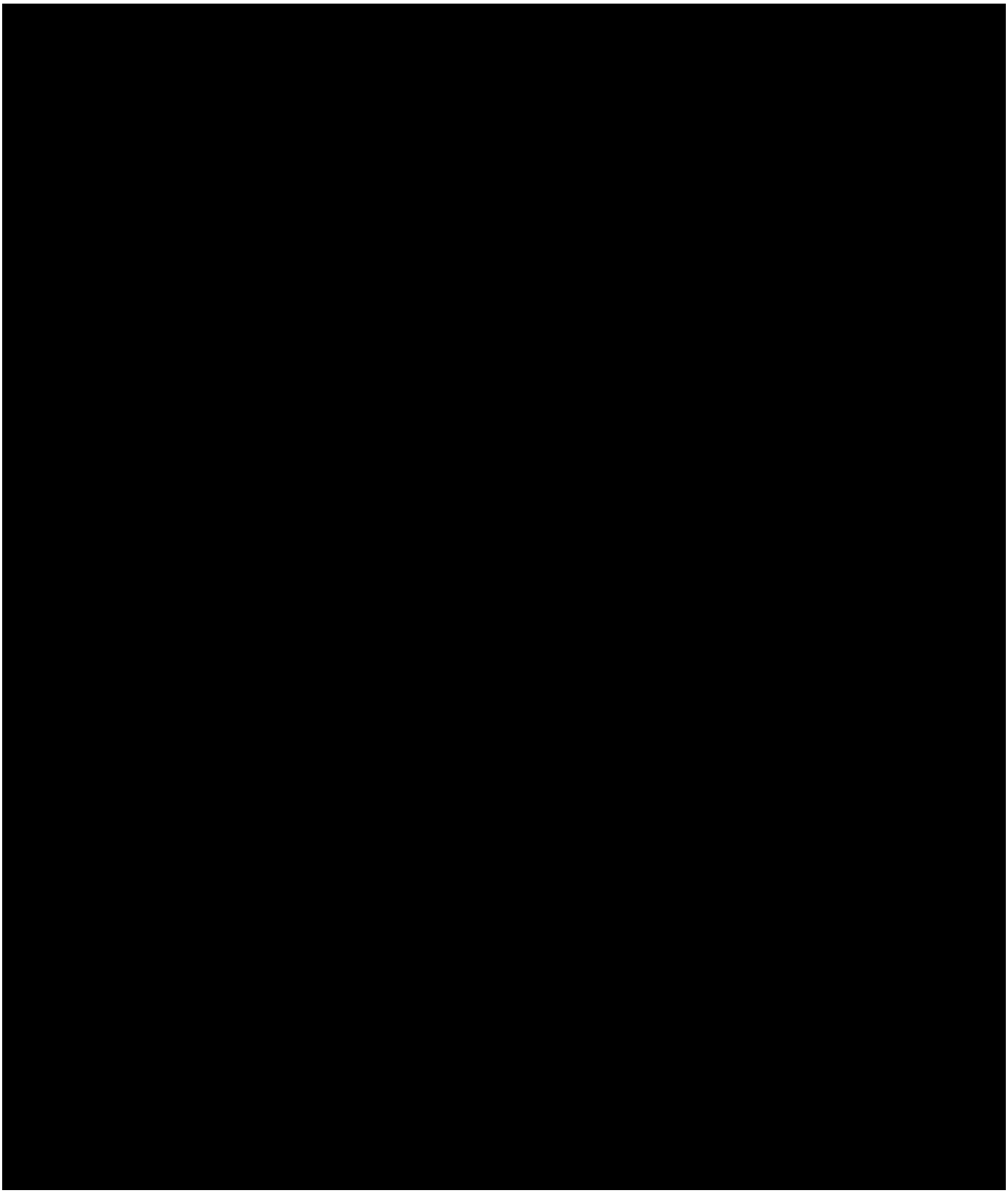
Please find below Carahsoft's supplemental information.

Carahsoft Technology Corporation

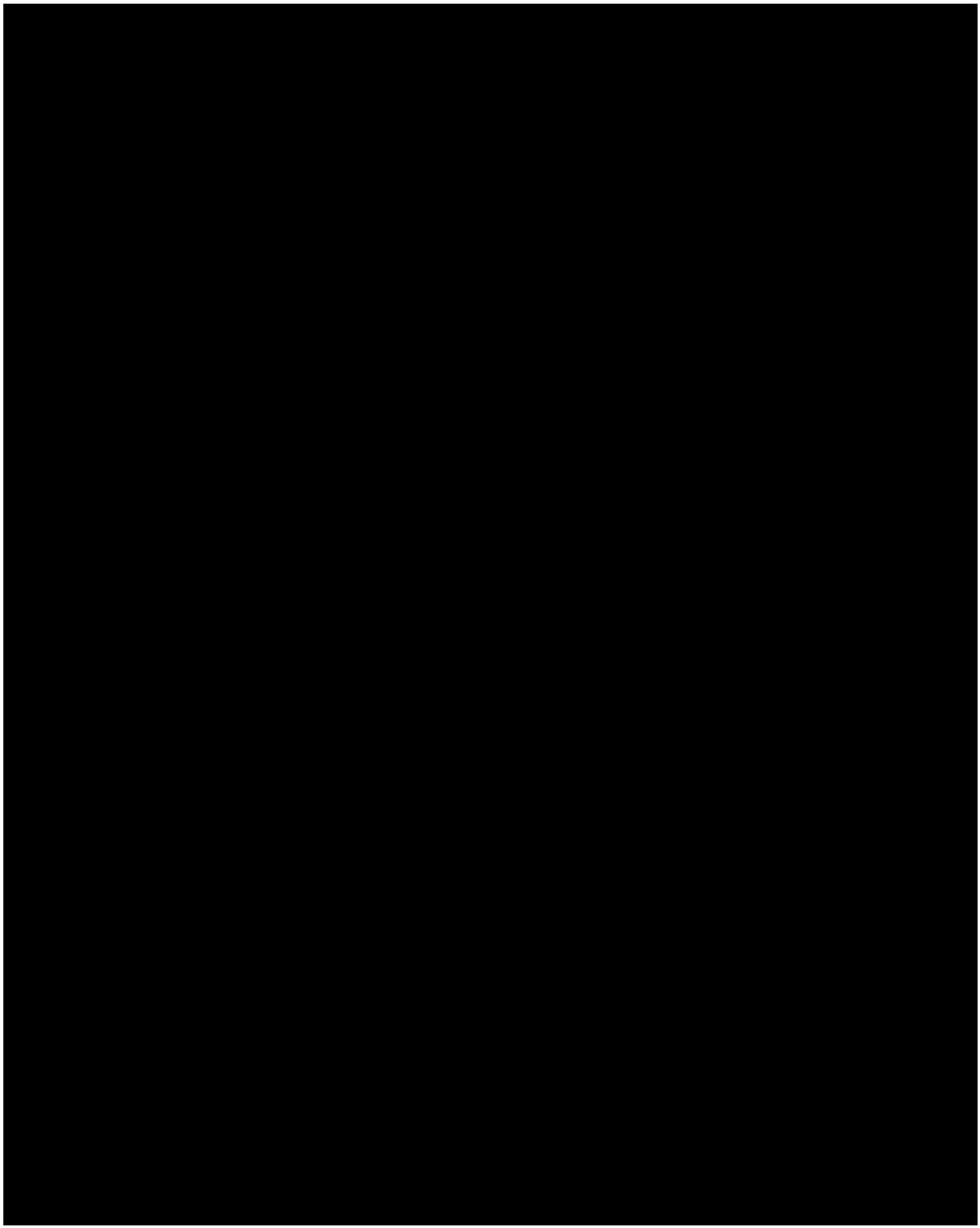
Financial Statements with
Independent Auditors' Report

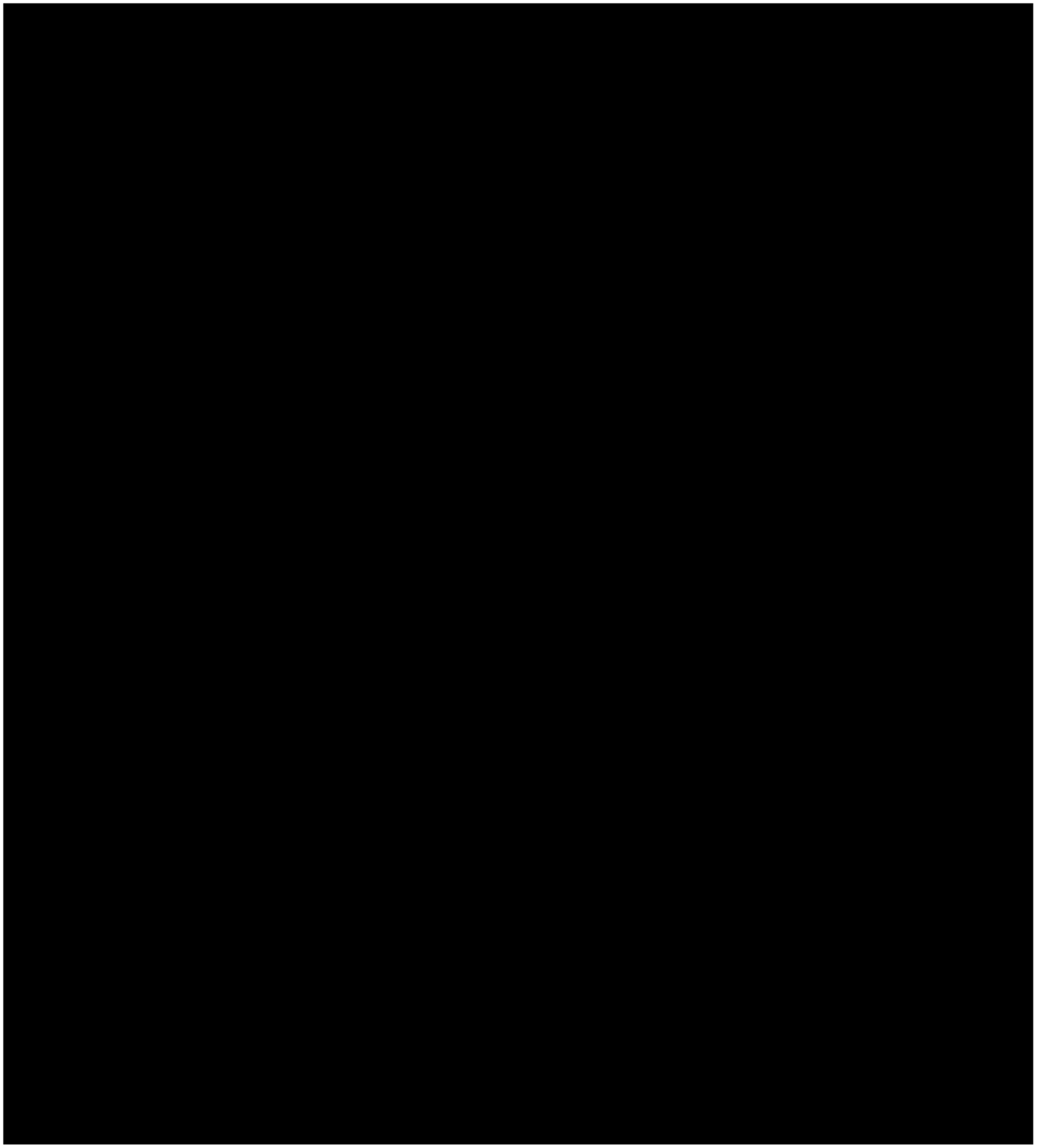
December 31, 2013

CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

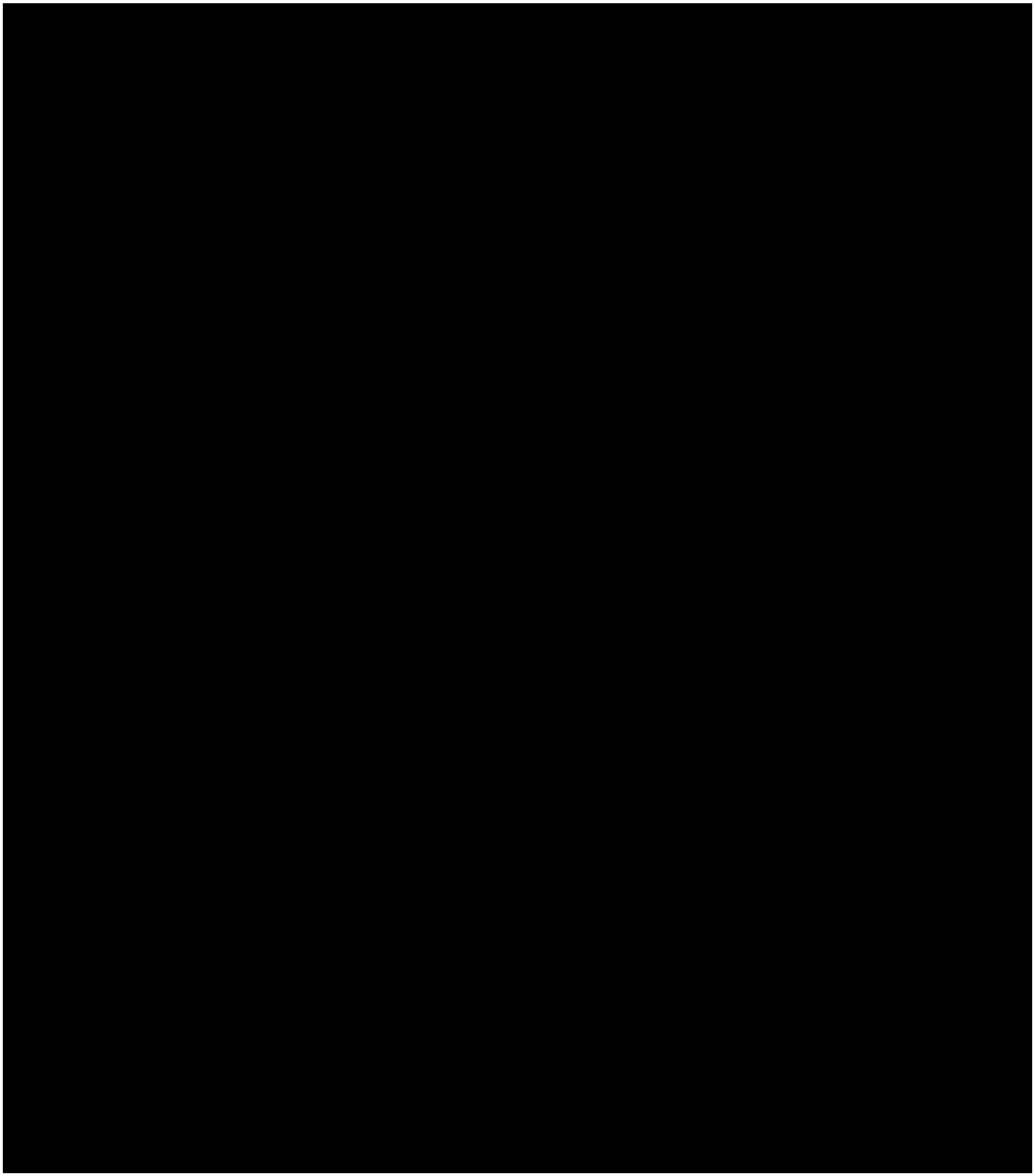




[redacted]

CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

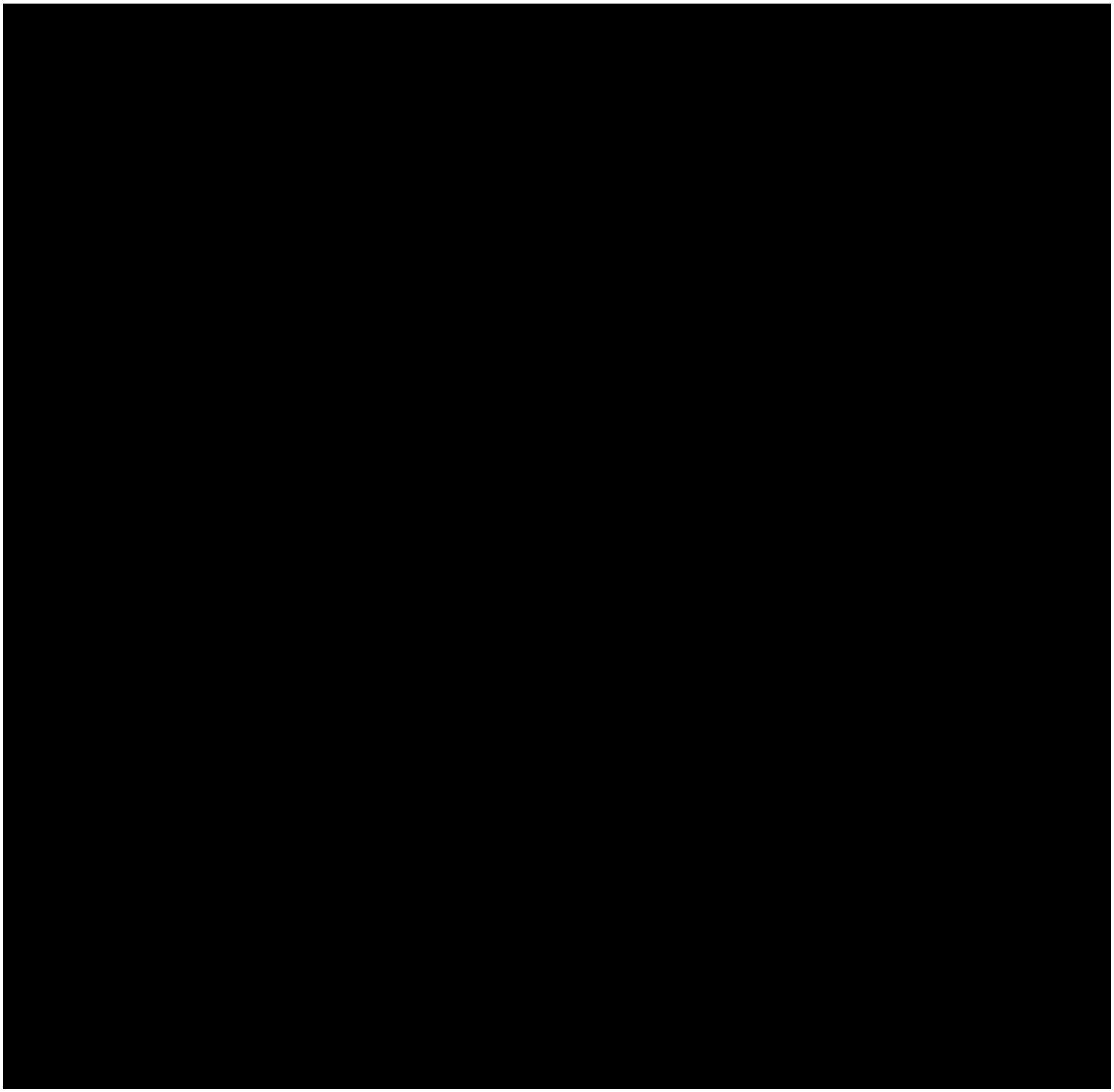


CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

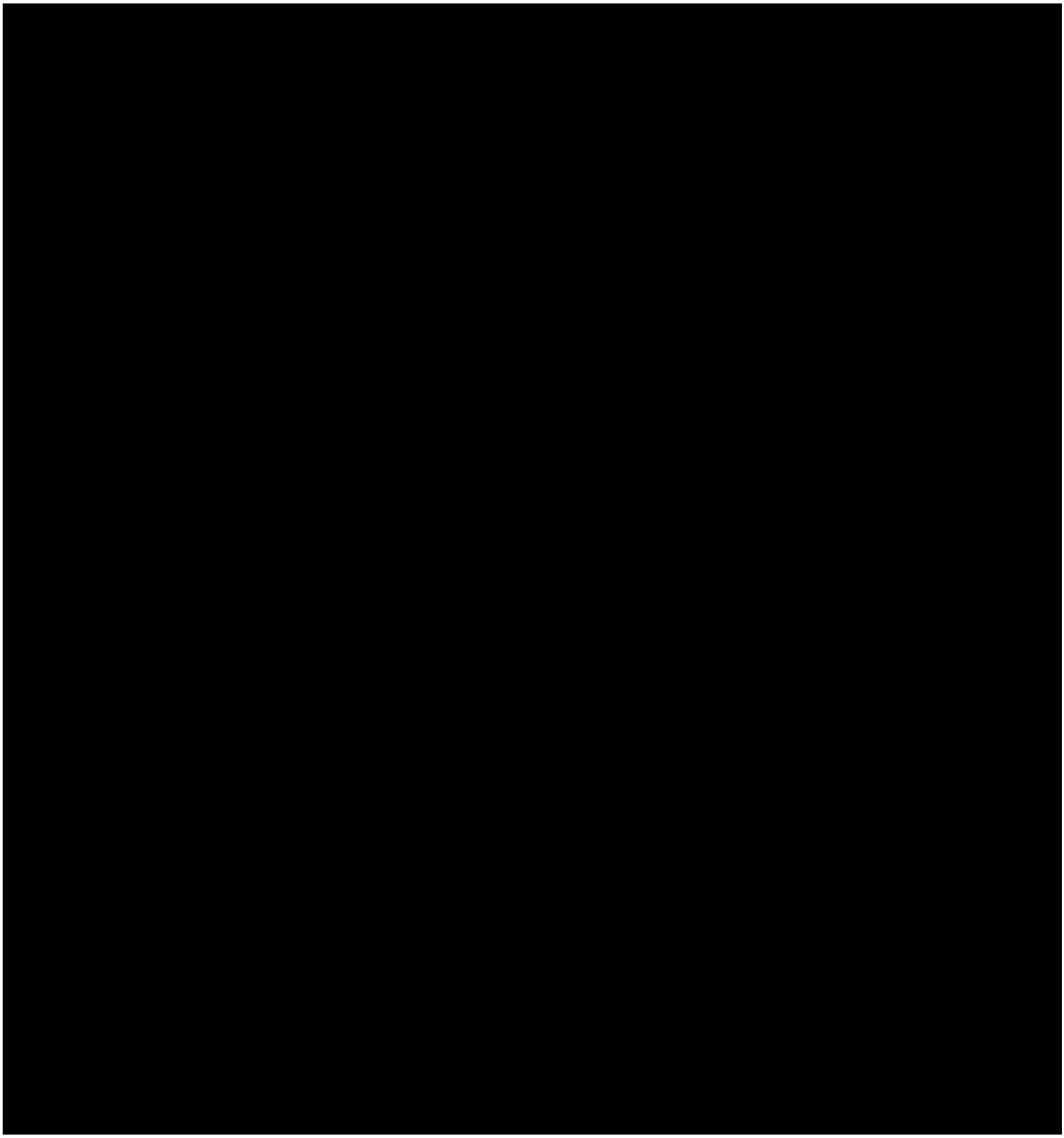
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

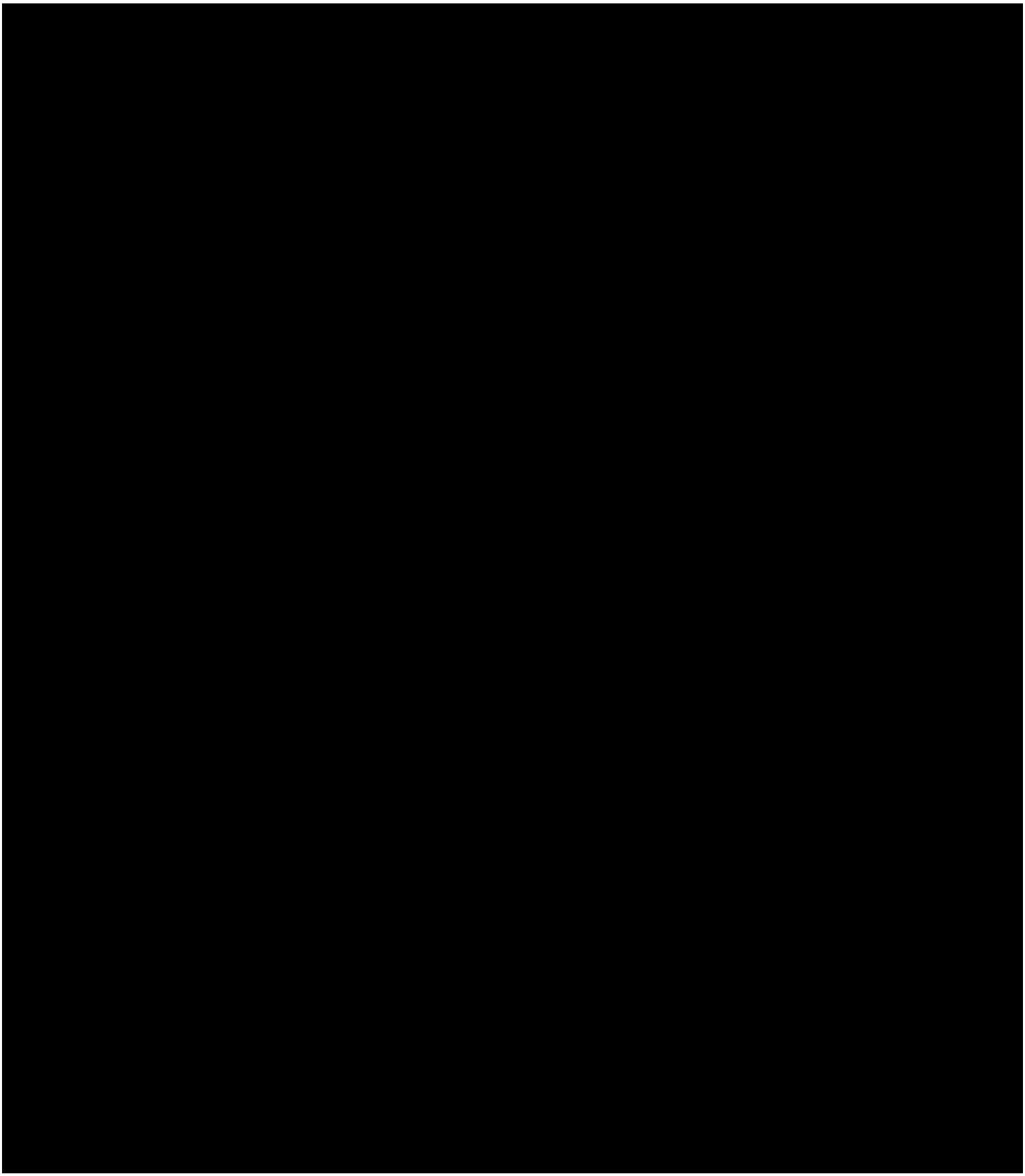


CONFIDENTIAL PROPRIETARY INFORMATION

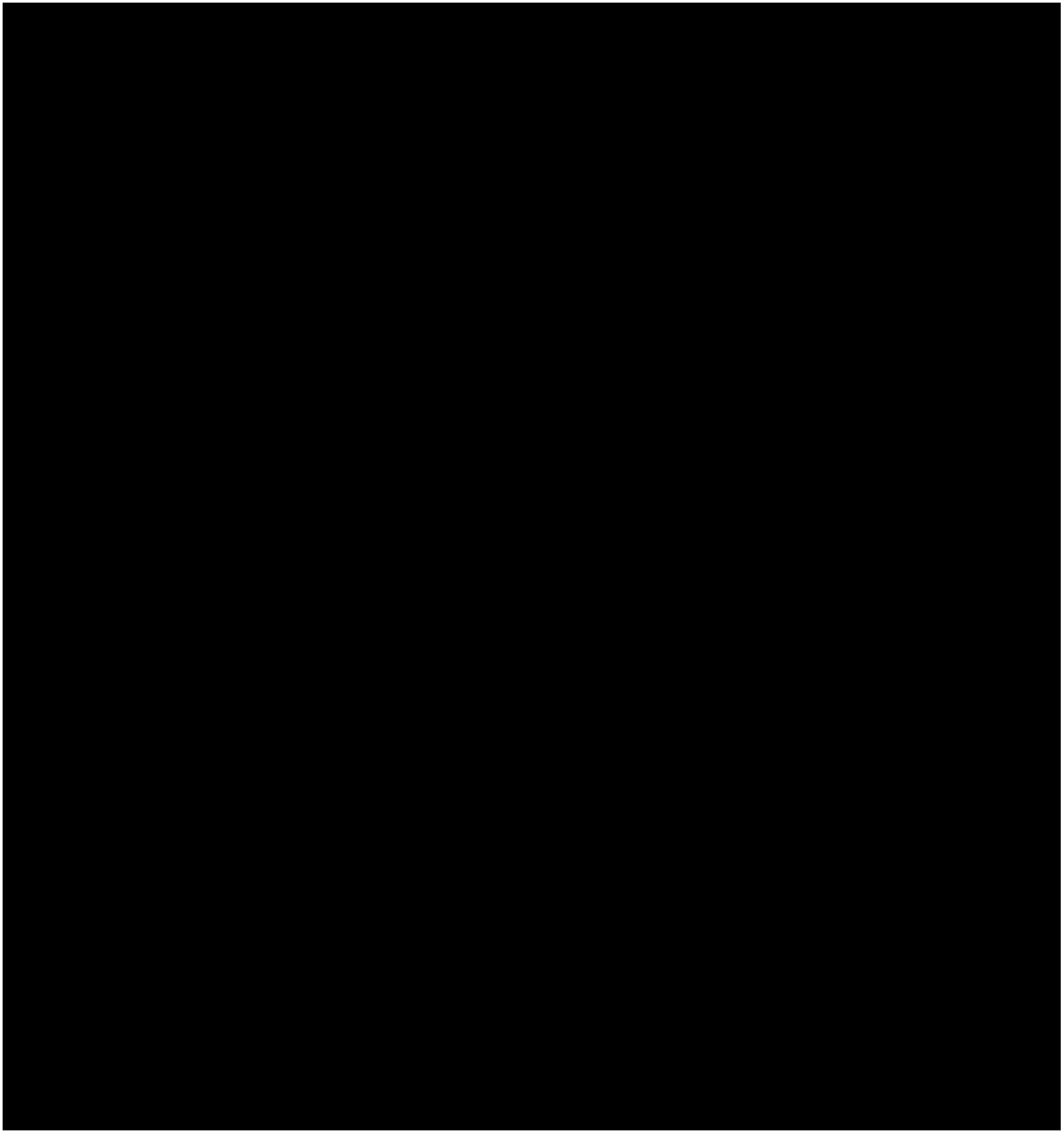
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

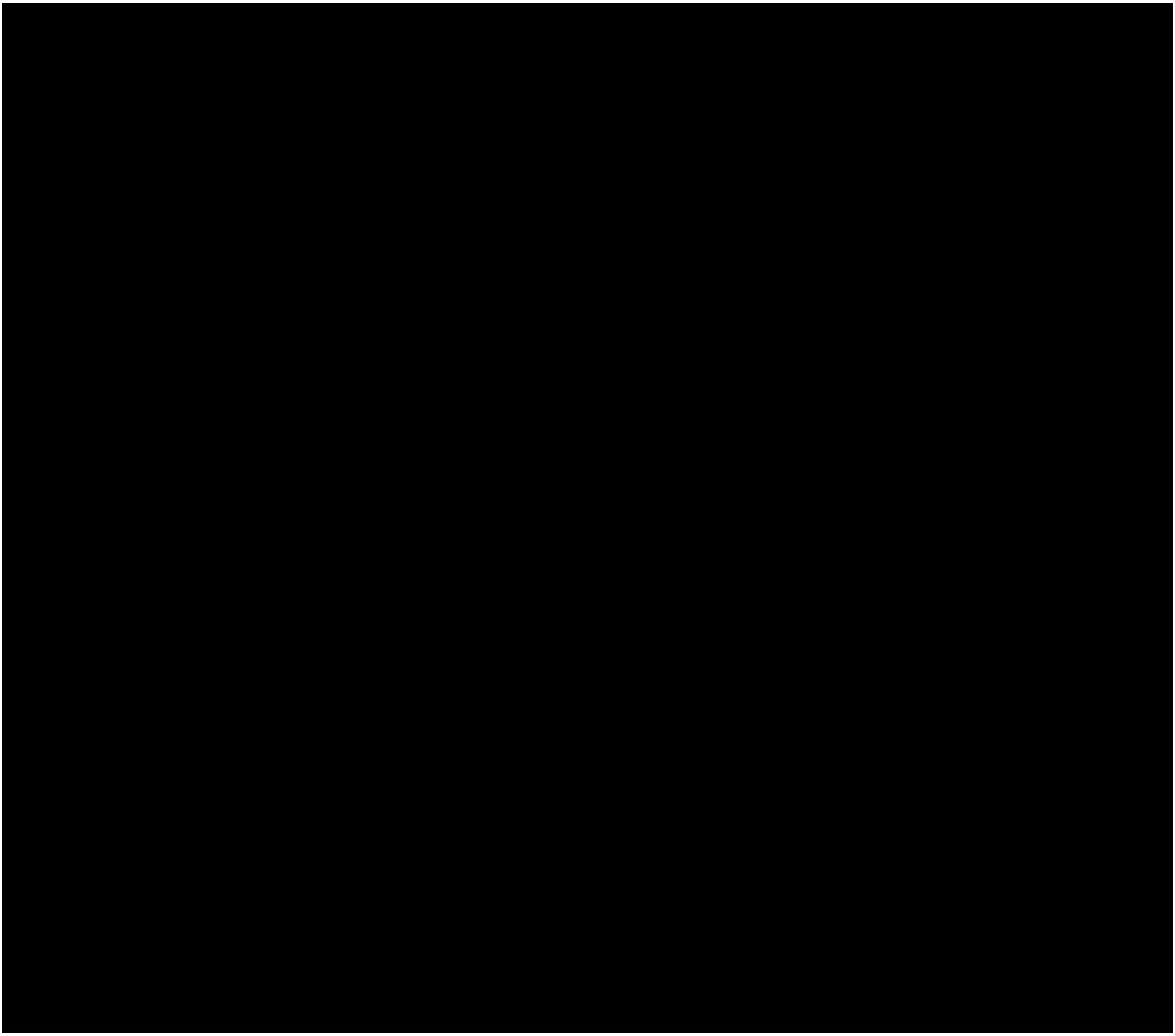
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

Carahsoft Technology Corporation

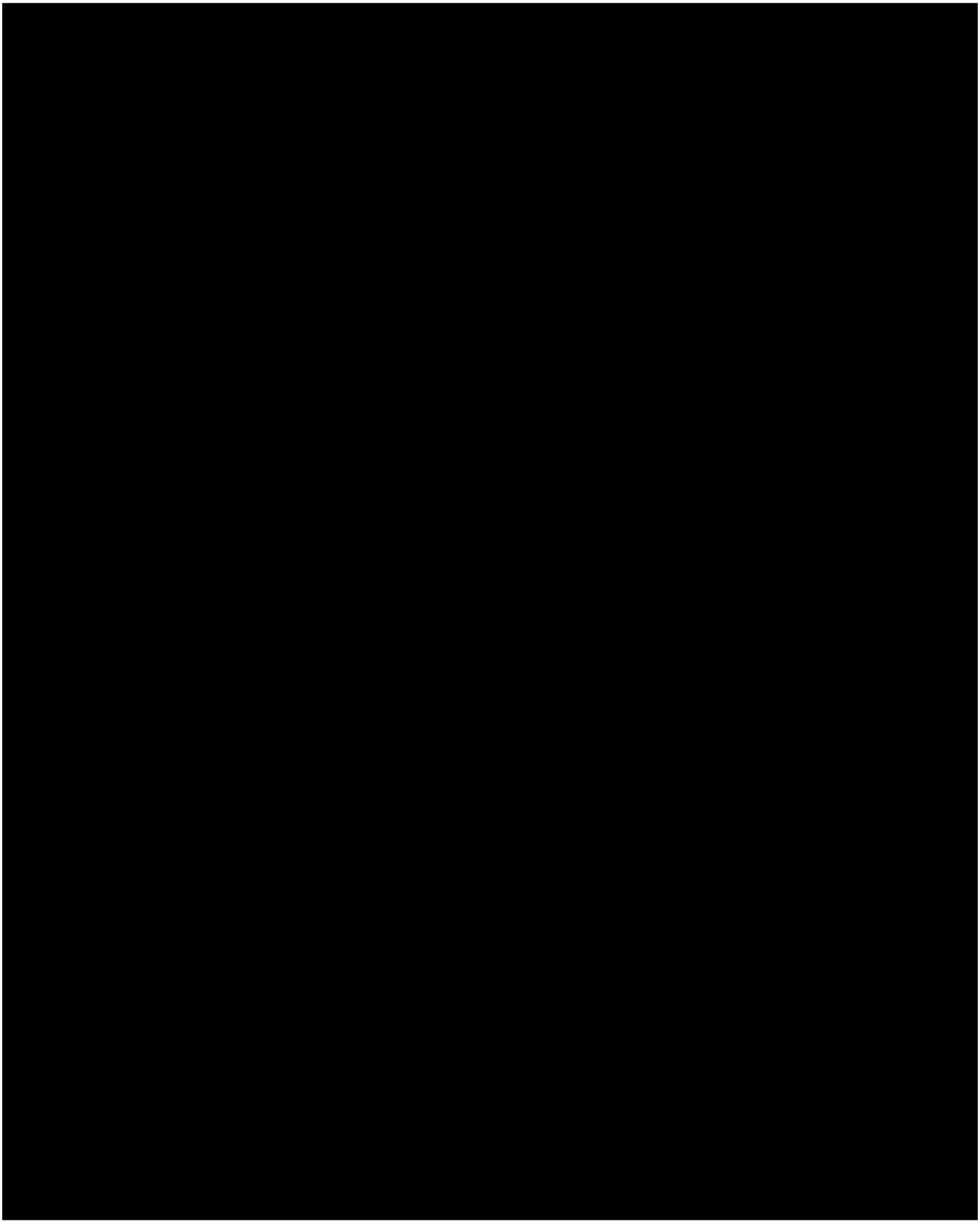
Financial Statements with
Independent Auditor's Report

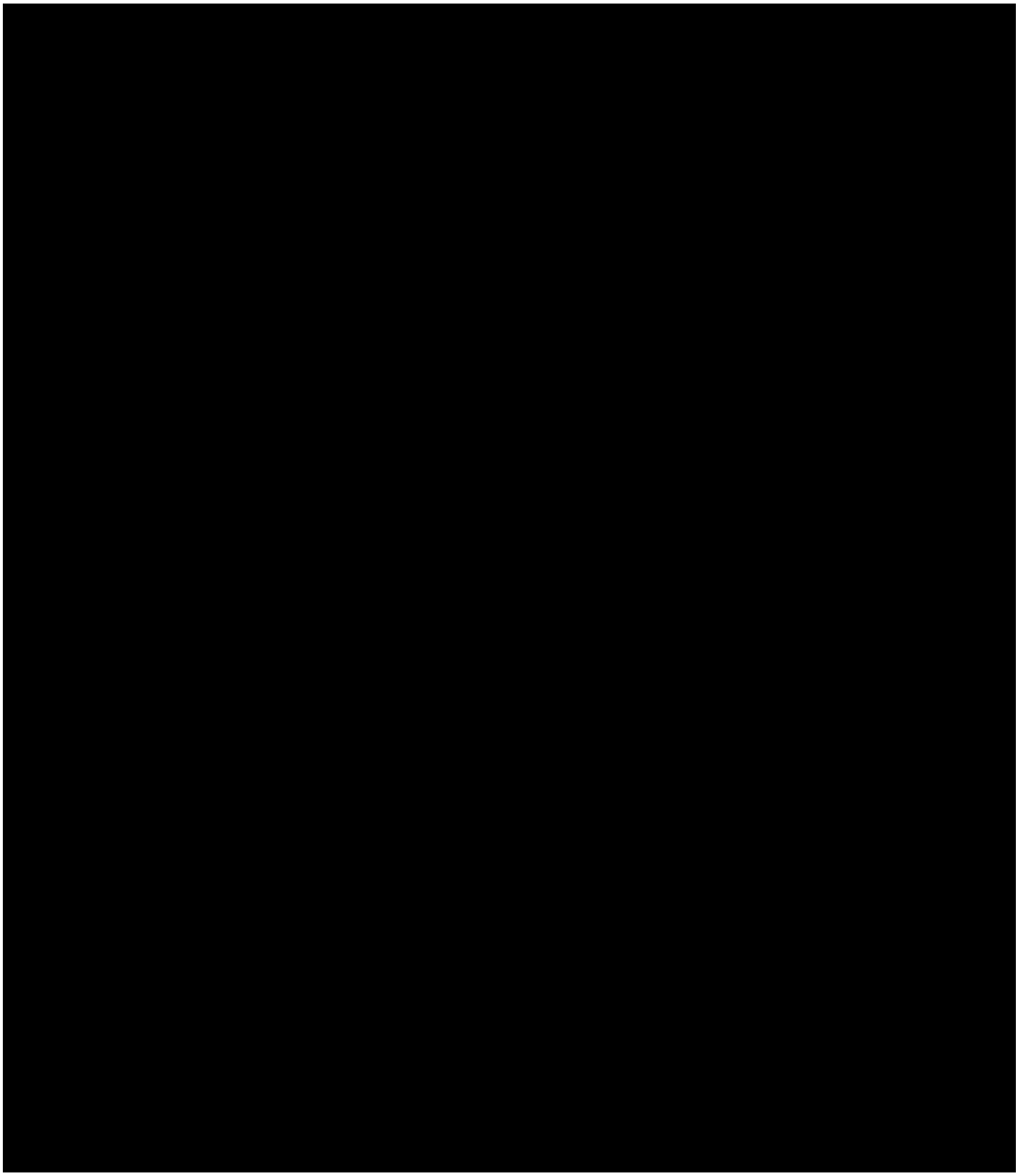
December 31, 2014

CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.





CONFIDENTIAL PROPRIETARY INFORMATION

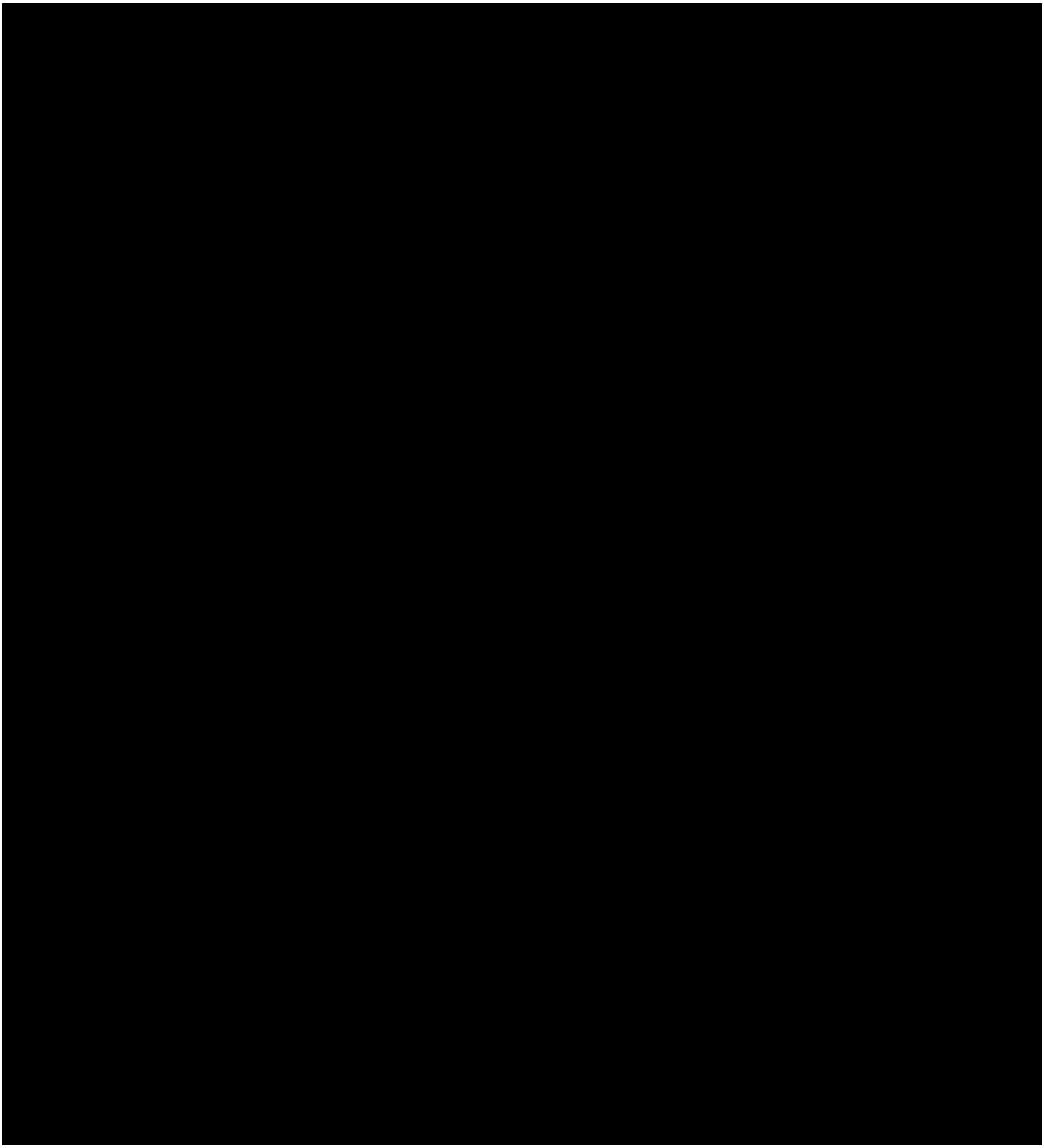
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

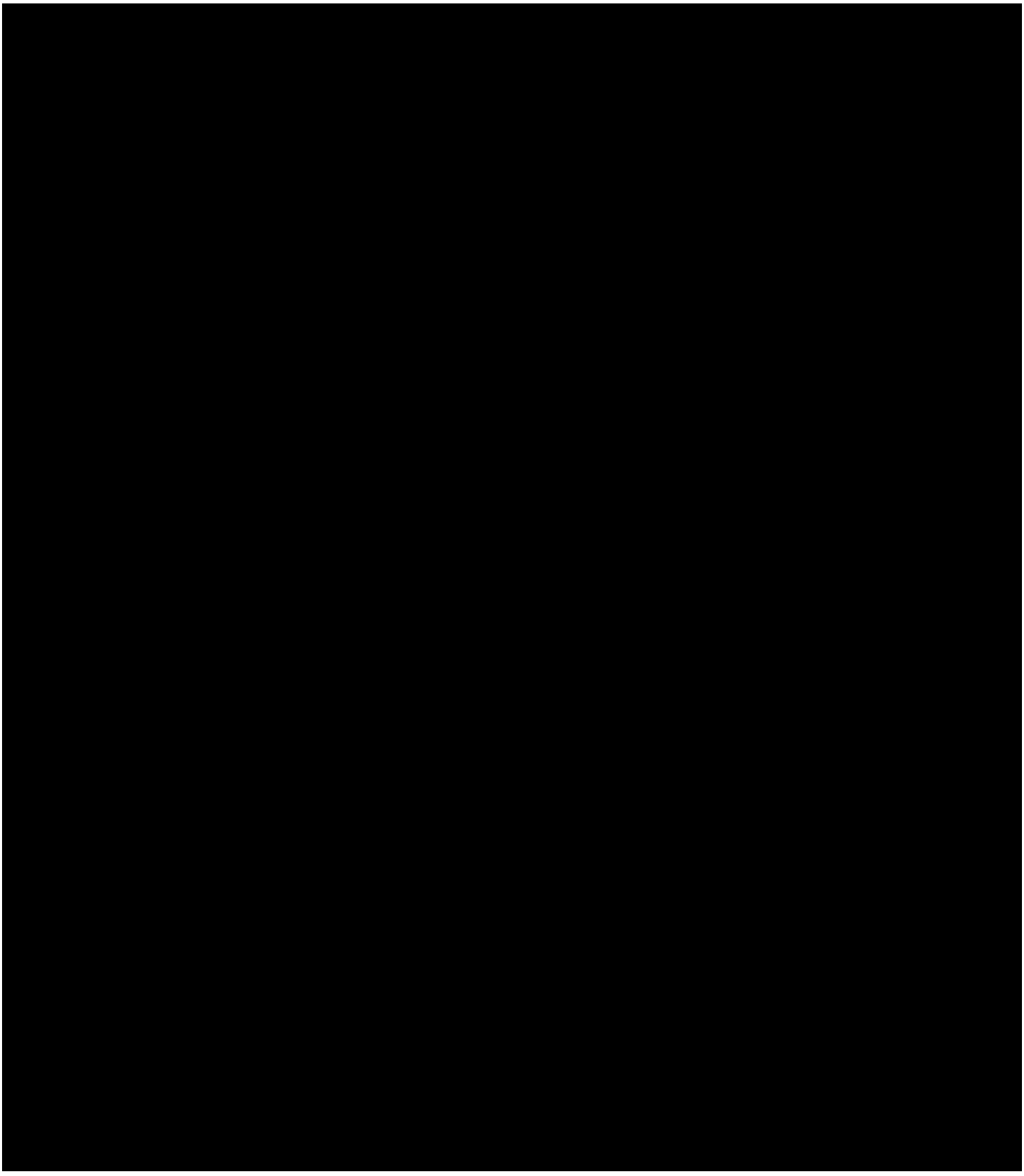


CONFIDENTIAL PROPRIETARY INFORMATION

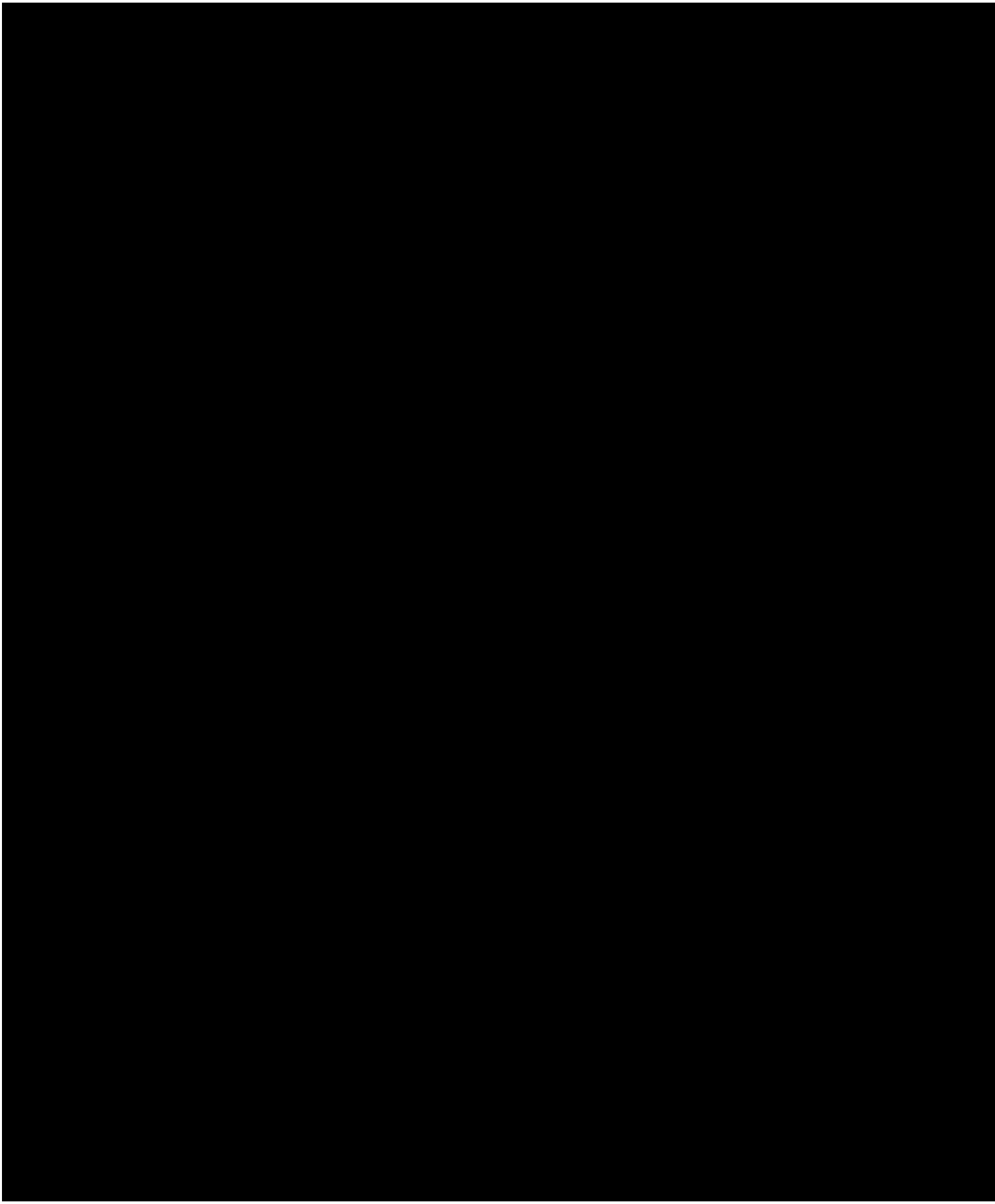
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

[redacted]

CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

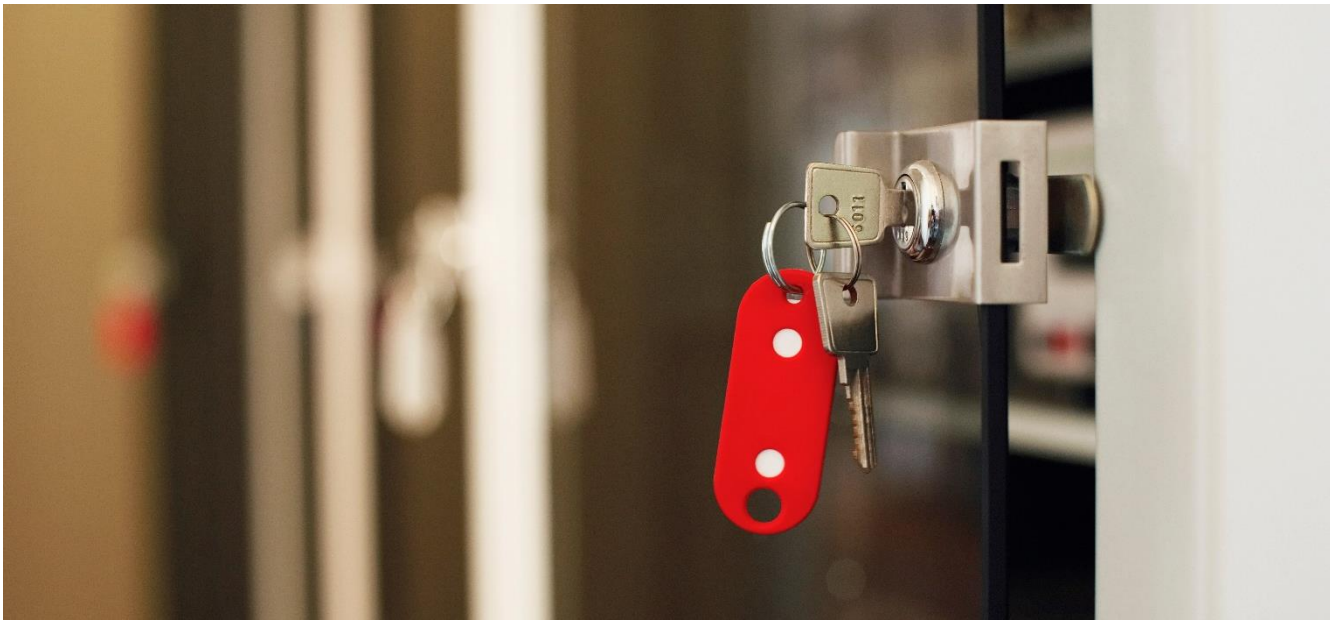


CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



SECURITY AND HOSTING OVERVIEW

June 2015

SAP Fieldglass

SAP

Table of Contents

1 INTRODUCTION 4

1.1 SCOPE OF OPERATIONS 5
1.2 SECURITY MANAGEMENT 6
1.2.1 SECURITY POLICIES, STANDARDS AND PROCEDURES 6
1.2.2 RISK MANAGEMENT 6
1.2.3 ASSESSMENTS 7
1.3 APPLICATION SECURITY 8
1.3.1 ENCRYPTION 8
1.3.2 DATABASE SEGMENTATION 8
1.3.3 DOCUMENT ENVELOPES 8
1.3.4 PAGE-LEVEL ACCESS CHECKING 9
1.3.5 URL ENCRYPTION 9
1.3.6 ACTIVITY LOGGING 9
1.3.7 APPLICATION TESTING 9
1.3.8 PASSWORD MANAGEMENT 10
1.3.9 EMAIL APPROVALS 10
1.3.10 APPLICATION PENETRATION TESTING 11
1.4 PHYSICAL SECURITY 11
1.4.1 INTERNET DATA CENTER CONSTRUCTION 11
1.4.2 ACCESS CONTROL 11
1.4.3 MAN TRAPS 12
1.4.4 KEY CONTROL 12
1.4.5 ALARM SYSTEM 12
1.4.6 CLOSED CIRCUIT TELEVISION SYSTEM 12
1.4.7 BACKGROUND CHECKS 12
1.4.8 HOSTING FACILITY SECURITY PERSONNEL 13
1.5 NETWORK SECURITY 13
1.5.1 REDUNDANT COMPONENTS 13
1.5.2 PRIVATE VIRTUAL LANS 13
1.5.3 FIREWALL 13
1.5.4 24/7 MONITORING 14
1.5.5 ENTERPRISE SIEM 14
1.5.6 NETWORK PEN TESTING 14
1.6 DATA MANAGEMENT 14
1.6.1 DATA BACKUPS AND REPLICATION 14
1.6.2 DATA ARCHIVING 14
1.6.3 DATA DELETION 15
1.6.4 DATA USAGE 15
1.6.5 DATA SCRUBBING 16
1.6.6 DATA ACCESS 17

1.6.7 DATA LOSS PREVENTION 18
1.6.8 CUSTOMER TERMINATION 18

2 RELEASE MANAGEMENT 19

2.1 RELEASE MANAGEMENT PROCESS 19

3 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN 21

3.1 DISASTER RECOVERY 21
3.2 BUSINESS CONTINUITY 21

1 Introduction

This document provides a general overview of the SAP Fieldglass security and hosting infrastructure. It is effective as of the revision date indicated below. However, as security needs continue to evolve, the specific information relating to the topics covered may be subject to change over time.

Security

The SAP Fieldglass solution was architected to be the most reliable and secure Vendor Management System available today.

SAP Fieldglass is proud to offer our customers, subject to review and acceptance by our audit partner, the following assurances:

- ISO 27001 certified since 2011
- SSAE 16/ISAE 3402 Type 2 SOC1 audits conducted since 2005
- SSAE 16 Type 2 SOC2 audits in the Trust Services Principles for:
- Security – the system is protected, both logically and physically, against unauthorized access
- Availability – the system is available for operation and use as committed or agreed to
- Processing Integrity – system processing is complete, accurate, timely, and authorized
- Confidentiality – information that is designated as “confidential” is protected as committed or agreed
- SSAE 16 Type 1 SOC2 audit in the Trust Services Principle for Privacy (Type 2 audit scheduled for Q3 2015)
- Annual third party pen testing of our network and application

This document provides an understanding of how SAP Fieldglass handles the following areas across its global operations:

- Scope of Operations
- Security Management
- Application Security
- Physical Security
- Network Security
- Data Management
- Release Management
- Disaster Recovery
- Business Continuity

1.1 Scope of Operations

SAP Fieldglass has global operations located in the following regions:

United States

Business office

SAP Fieldglass
111 N. Canal Street
Suite 600
Chicago, IL 60606

Active and passive datacenters

Century Link 2425 Busse Road Elk Grove Village, IL 60007	Equinix / ServerCentral 1735 Lundy Avenue San Jose, CA 95131

APAC

Business office

SAP Fieldglass
Suite 5, 48 Lovett Street
Manly Vale
NSW 2094
Australia

European Union

Business office

SAP Fieldglass
One Valentine Place
London
SE1 8QH
United Kingdom

Active and passive datacenters

ServerCentral c/o Equinix Laarderhoogtweg 57 1101EB Amsterdam, Netherlands	ServerCentral c/o Telehouse North 14 Coriander Avenue London E14 2AA United Kingdom

The terms "active" and "passive" designate which of the production hosting environments is being used as the primary (active) and which is being used as the backup (passive or disaster recovery). These designations are not static and SAP Fieldglass will occasionally fail over the active hosting environment to the passive hosting environment. This practice ensures that SAP Fieldglass is capable and ready in the unlikely event a disaster occurs and we need to fail over to the passive site.

1.2 Security Management

SAP Fieldglass' Security Team is responsible for implementing and maintaining the security controls to ensure that SAP Fieldglass information systems are secure. SAP Fieldglass has based its security program on industry standards and best practices. For our established datacenters, these practices are audited annually by a third party with results available to customers in October.

1.2.1 Security Policies, Standards and Procedures

SAP Fieldglass maintains a comprehensive set of policies that define the information security goals and objectives. Each policy may be supported by a standard that dictates the required security requirements to ensure the uniform application of technologies and processes.

1.2.2 Risk Management

SAP Fieldglass manages risk by the identification of threats and vulnerabilities to its information systems and through a control selection process. Controls selected fall into the following categories:

- Policy
- Physical and Environmental Security
- Organizational Security
- Communications and Operations Management
- Acceptable Use
- Access Control
- Third Party Access
- Information Systems Acquisition, Development and Maintenance
- Asset Management
- Incident Management
- Personnel Security

- Compliance

As an element of our ISO 27001 compliance, SAP Fieldglass conducts an enterprise-wide risk assessment. Key individuals from every department are interviewed so that risks can be identified. Risks are then evaluated and entered into a risk treatment plan. This plan is managed by the Security team with oversight by the Security Steering Committee. The Security Steering Committee meets on a quarterly basis.

1.2.3 Assessments

SAP Fieldglass periodically assesses the security controls to review the effectiveness of each control in addressing risk. If SAP Fieldglass' assessment suggests a need for changes, the baseline standard may be changed to include additional controls.

Internal Audit

SAP Fieldglass conducts quarterly internal audits for critical controls. Evidence is reviewed by our Sr. Compliance Analyst and a formal assessment report is prepared. Failed controls are made visible by this process so they can be remediated. Executive sign off on the internal audit reports is required.

External Audit

SAP Fieldglass also contracts with third parties on an annual basis to perform formal security audits on the following:

- ISO 27001 surveillance audit
- SSAE 16/ISAE 3402 Type 2 SOC1 audit
- SSAE 16 Type 2 SOC2 audits in the Trust Services Principles for:
- Security
- Availability
- Processing Integrity
- Confidentiality
- SSAE 16 Type 1 SOC2 audit in the Trust Services Principle for Privacy (Type 2 audit scheduled for Q3 2015)
- Network penetration test
- Application penetration test

These assessments allow SAP Fieldglass to maintain an appropriate security posture in order to protect the company and its systems, as well as its customers' data.

We are currently working with our third party audit partner in bringing our EU datacenters into scope for our 2015 ISO 27001 audit and SSAE 16/ISAE 3402 Type 2 SOC1 and SOC2 examinations.

1.3 Application Security

Our application provides application-level security through a combination of encryption, page-level access checking, document envelopes, and activity logging. Application security is handled through a combination of programming checks, application server configuration, and database server configuration. SAP Fieldglass uses 128-bit SSL (HTTPS) encryption for all data transmissions over the public Internet, including data shared between the product and end users and data shared between the product and back-end systems.

Passwords are encrypted using a one-way hash with salt based on the SHA-256 encryption algorithm. The hash value is saved within the database; not the password.

The base SAP Fieldglass application does not require data that would require breach notifications if compromised. If the customer chooses to store sensitive data, custom fields may be defined by the customer that can be encrypted with AES-256. These fields can also be optionally masked from view while entering and viewing the fields in the application.

1.3.1 Encryption

By default, the application utilizes SSL encryption for all data transmissions over the public Internet.

In addition, the SAP Fieldglass hosted application encrypts sensitive data stored on the database so that only properly authorized users (or systems) will be able to decrypt the data. Because no state information is stored on the application server, in the unlikely event of unauthorized access to the database, the sensitive data is still encrypted.

1.3.2 Database Segmentation

SAP Fieldglass is a SaaS and utilizes a multi-tenancy database. Each customer is assigned a unique company code. Every record written to the database is keyed using this company code. After a user authenticates into the system, a session ID is generated which holds vital information about the user including their company code, user role, and data visibility restrictions. The session ID is cached server side to eliminate any ability for a malicious user to modify its contents.

1.3.3 Document Envelopes

Throughout the system, there are a number of events that generate “documents.” These are digital representations of their real-world counterparts. For example, job postings, work orders, time sheets, and invoices are all represented in the system as documents.

Each document in the system has an accompanying digital envelope that stores all access to that document. For example, when a job posting is created, an envelope entry is added for creation that records the date, time, and person. When it is submitted, another entry is added recording the date, time, and person.

1.3.4 Page-Level Access Checking

The application has been designed so that every single web page checks for access rights before displaying itself. Additionally, each page performs a second check to ensure that an authorized user will only have access to those data elements and functionality that has been expressly authorized by the system administrator.

The post-authentication session ID that is generated and cached server-side is validated prior to showing each page. SAP Fieldglass stores a non-persistent cookie in the browser and compares back to the server-side session ID. If they no longer match due to malicious activity, the user is redirected to a "You are not authorized" page.

Authorization is handled through the use of user-defined User Roles. User Roles provide the customer, through its designated administrators, the flexibility to specify the type of access given to a member of that user group based on the definitions configured by the administrator. The User Role controls what areas of the application are accessible to the user group and what actions they can perform in those areas (e.g. job posting create, time sheet approve, etc.).

1.3.5 URL Encryption

SAP Fieldglass does not pass any sensitive data in its URL query strings. Parameters that are used to identify users in the system are protected by anonymizing the field variable and then encrypting the associated value using AES-256.

1.3.6 Activity Logging

As users access the system, all of their business significant activities are tracked and logged including failed login attempts, successful logins, approvals, submissions, etc. This activity log provides a full audit trail of what actions a particular user performed within the system and the timestamp as well.

1.3.7 Application Testing

Upon request, SAP Fieldglass will provide customers with a sandbox environment where system testing can occur outside of production. This is useful when testing out configuration changes, new integrations, and/or new reports prior to making the changes live in the customer's production instance.

Upon request, customer's data can be anonymized. SAP Fieldglass has the ability to scrub the data such that it is unrecognizable. Data element replacement is accomplished by an automated SAP Fieldglass utility that replaces the customer's company code, user names, business units, cost centers, and sites from a store of random variables. Any or all of these elements may be chosen for replacement.

Sensitive data that has been designated by the customer to be stored in the SAP Fieldglass application is encrypted with AES-256. The encryption and decryption keys are different between production and test environments and are different between the US and EU datacenters. These keys are stored in the corporate password vault and are accessible only by the Database Administrators and the Lead Architect.

Once customer testing has been completed, the Environment Management team (a team within Professional Services) destroys the environment. The database is purged and the VM is returned into circulation.

1.3.8 Password Management

The SAP Fieldglass application provides each customer the ability to define a Password Policy. This policy contains custom-defined password rules that each user in the customer's instance must adhere to. The policy provides 20 different password rules such as minimum length, user lockout preference (hard lockout vs. time-based reset), days to expiration, minimum password age, etc. Also included is the ability to specify a regex pattern(s). This pattern dictates the password value syntax that each user must follow.

When customer chooses to use a test instance ("sandbox"), all user password values remain unchanged from their production values. All passwords and visibility restrictions remain unchanged to ensure that users in the test instance are not able to gain access to data they're not privileged to see in production. Also, the password policy that is enforced in in the production instance is also enforced in the test instance.

New user invitations are sent via email. Recipients enter their 1-time passcode and are then forced to specify a new password that complies with the customer's password policy rules. User invitations expire after 21-days.

1.3.9 Email Approvals

In order to better support our growing mobile workforce, SAP Fieldglass offers customers a supplementary method for approving their work items. Via email, approvers are able to submit their approval or rejection response by simply replying to the approval work item that was sent to them. This method has been proven to reduce approval cycle times by several days since the approver does not have to be in the office. This feature has been architected with the following security controls:

- Only the original recipient can approve/reject the work item. If the recipient forwards the email to another person, the system will not accept the response.
- Email spoofing is not a risk. A unique ID is generated for each approval request. This unique ID along with the person ID of the intended recipient is stored encrypted with AES-256. So even if the email address sending the approval/rejection response is legitimate but the sender is not, the system will detect this anomaly and not accept the response.
- A SAP Fieldglass approver can identify another user as their Proxy and/or Delegate when they will be out of the office and unable to handle the approval requests. By design, neither of these roles receive approval work items via email. So only the original recipient can ever submit an approval/rejection response via email.
- If the customer created custom fields where sensitive information is stored encrypted, those fields and associated values are not allowed to be selected for inclusion in these email approval notifications.
- The system audit trail is updated with all user actions including approval/rejection activities via email. This audit trail is accessible by privileged customer users and can be used to monitor user activity.

In order to compromise the security of our email approval feature, a malicious user would need to hack into another user's email account, locate the SAP Fieldglass approval request email, and then submit the approval/rejection response.

1.3.10 Application Penetration Testing

SAP Fieldglass uses a combination of manual and automated testing to ensure the application is secure. Various automated commercial tools are used prior to each major release of the SAP Fieldglass system (three times per year).

On an annual basis, SAP Fieldglass engages a 3rd party security company to conduct pen testing services against our application. This is in addition to SAP Fieldglass' own internal penetration testing efforts.

SAP Fieldglass has several test environments available for customers to conduct their own application penetration testing if requested.

1.4 Physical Security

The SAP Fieldglass data center provides physical security through its secure hosted facilities. The application is hosted within a secure unmarked cage. SAP Fieldglass manages everything from the cage in. Meaning, SAP Fieldglass manages all servers, devices, and software in the cage. The hosting provider provides physical security, internet connectivity, and HVAC.

1.4.1 Internet Data Center Construction

Exterior perimeter walls, doors and windows are constructed of materials that afford UL Standard #752, Level V Ballistic Protection.

1.4.2 Access Control

The data center uses an Access Control System (ACS), which supports a networked card reader and alarm system. The ACS uses proximity card readers to control access into perimeter doors, shipping/receiving areas, storerooms and other areas. Biometric hand scanners are installed to control access into the network control center, telecommunications node room and customer vaults. Additional access control measures include:

- Designated with signage as controlled access areas
- Areas within the internet data center are designated as restricted
- Access into the internet data center and restricted areas is controlled by biometric hand scanners, and is limited to authorized personnel
- Card access badges or contractor/visitor badges are required to gain entry
- All employees, customers, vendors, contractors and visitors must be sponsored by a facilities pre-approved sponsor to gain access
- Visitors are escorted at all times within the controlled access area perimeter

1.4.3 Man Traps

The system includes the following key features:

- Anti-passback
- Integrated metal & explosive detection
- Video monitored / recorded
- Two-way intercom audio to Security Control Room
- Level V ballistic protection
- Weight sensors limit entry to one person at a time (no tailgating)
- ADA compliant
- Intrusion / tampering alarm monitoring by Security Control Room
- Integrated card access & biometric access control systems limits access to persons verified by hand geometry
- All systems are supported by redundant power management system (generators).

1.4.4 Key Control

Facilities security staff is the custodian of all security and cage keys. These keys are maintained and tracked through a comprehensive issue, retrieval, audit, and storage process. The listing of all customers, customer employees and cage assignments is updated in real-time maintained to ensure that cage access is restricted to authorized personnel.

1.4.5 Alarm System

The ACS is used to monitor and log security alarms. The ACS monitors all:

- Perimeter doors
- Restricted Area doors
- Shipping / receiving doors

1.4.6 Closed Circuit Television System

Facilities employ an extensive closed circuit television system to monitor the exterior and interior of the internet data center. Exterior cameras provide views of critical support equipment and perimeter doors. Interior cameras are positioned to monitor all internet data center aisle ways, requests for entry and entry into the internet data center, shipping / receiving areas, high-security vaults and the internet data center lobby. All cameras are recorded on digital video recorders 24 x 7.

1.4.7 Background Checks

SAP Fieldglass requires background checks be performed at the time of hiring on all personnel. These background checks are performed by a nationally recognized third party company. SAP Fieldglass initiates the background check request for all potential employees and independent consultants. If the independent contractor is placed through

an agency, the agency will conduct a background check and confirm with Human Resources whether the results were completed with/without discrepancies. If the independent contractor is placed directly, SAP Fieldglass will conduct the background check.

Background checks include the following:

- Social Security Trace
- Statewide & National Criminal Report (7 years)
- Sex Offender Registry & Terrorist Watch
- Compliance Authorities Database Checks – Global (OFAC level verification)
- Education verification
- Employment verification (7 years)
- Global Sanctions & Prohibited Parties
- Credit (only for specific finance roles)

1.4.8 Hosting Facility Security Personnel

The security office duties include:

- Response to calls for assistance
- Security facility inspections
- Fire and safety patrols
- Shipping / receiving security
- Physical security audits and assessments

1.5 Network Security

The SAP Fieldglass network infrastructure includes redundant components, firewalls, and 24/7 monitoring.

1.5.1 Redundant Components

Most network components are internally redundant. For example, routers have redundant power supplies; servers have redundant drives, power supplies, and NIC cards. Additionally, all network components are redundant to provide redundancy and security in the event of a component failure.

1.5.2 Private Virtual LANs

The application network architecture has been designed with multiple private virtual LANs using redundant Cisco routers. Every major network layer is placed on its own virtual LAN with rules about which protocols and ports are accessible.

1.5.3 Firewall

SAP Fieldglass has implemented dual-vendor redundant firewalls between the public internet and the SAP Fieldglass private network, as well as between each virtual LAN. This

firewall has been configured to enforce protocols and ports that are able to cross LANs with a default deny stance.

1.5.4 24/7 Monitoring

SAP Fieldglass provides 24/7 monitoring of suspicious activity. Any failure is promptly reported and, after an initial analysis, escalated to the next appropriate level.

1.5.5 Enterprise SIEM

Our security incident and event management (SIEM) tool has been configured to collect logs and events from all systems and devices within the SAP Fieldglass network. Forwarders are used to collect, filter, normalize and forward relevant data to an Indexer. Each installation listens for Syslog data and actively pulls WMI information from its respective environment. Security related issues are monitored and alerted on where required.

1.5.6 Network Pen Testing

On an annual basis, SAP Fieldglass engages a 3rd party security company to conduct pen testing services on our network.

1.6 Data Management

1.6.1 Data Backups and Replication

SAP Fieldglass has a highly available backup solution that guarantees data can be restored as expediently as possible. Our solution performs a continuous replication of data to our passive production hosting facility. SAP Fieldglass takes incremental SQL backups every 15 minutes and full backups on a nightly basis. Backups are transferred to the passive production hosting environment over a secure channel. SAP Fieldglass' solution offers continuous protection of customer data geographically without imposing performance degradation or scaling limitations. Data is encrypted both at rest and in transit with AES-256.

Data backups and replication are performed between the active and passive production environments. The US-based active production environment replicates data to the US-based passive environment. Likewise, The EU-based active production environment replicates data to the EU-based passive environment.

Also refer to section 3.1 Disaster Recovery.

1.6.2 Data Archiving

Data is archived throughout the year. Eligible transactional and reporting data are moved from the active database to an archive database after 24 months. Archived data can be accessed only by customer users with a user role of Administrator. Archive data is accessed using the same login screen and user interface that is used to access current data. Reports can also be generated using archive data from the standard interface.

The criteria for archiving data are as follows:

- Data remains in the active database for 24 months, at which point eligible data is moved to the archive database.
- Data remains in the active report database for 24 months, at which point eligible data is moved to the archive report database.
- Archiving begins with the worker. When a worker's end date is more than 24 months old, the worker and all associated data including the worker's work orders, job seeker record, job posting, time sheets, expense sheets, and payment-related items such as invoices are archived.
- The archive process is run as a batch job on a weekly basis to move data from the active databases to the archive databases.
- Data cannot be moved back from the archive database to the active database.

SAP Fieldglass does not delete data from its archive databases and has data older than 7 years. In the future, if SAP Fieldglass decides to delete archived data, we will ensure that a minimum 7 years of data is retained.

1.6.3 Data Deletion

Data deletion occurs only when required by a customer. SAP Fieldglass' data deletion capabilities allow customers to remain compliant with data privacy, data protection, and other related data directives.

- Deletion logic is based solely on a customer's business requirements. A custom script is developed by SAP Fieldglass.
- Results are verified in a non-production environment by both SAP Fieldglass and the customer prior to executing in production.
- A "Preservation" flag is available for use. Customers can set this flag on any data to override logic that would otherwise delete the data. This is useful during times when litigation or eDiscovery efforts are in progress and certain data must be preserved.
- Script execution frequency is determined by the customer.

SAP Fieldglass is contractually obligated to retain at least 7 years of data for customers.

1.6.4 Data Usage

Customer data is required in non-production environments for various reasons:

- Second level help desk support for customer defect investigation and resolution.
- Supporting customer requests for updating data, whether it be for desired changes or corrections for data modified by the customer in error.
- Customer sandboxes – these are non-production environments configured only with the customer's data (customer's data is "sliced" out from the multi-tenancy production database). These sandboxes are required for many

reasons, including testing of new or changed integration connectors, reports, and/or application configuration changes such as revised approval workflows. New application features can also be turned on and reviewed in the sandbox before turning on in the live production instance.

- Any data deletion scripts that are developed between the customer and SAP Fieldglass must be tested in a non-production environment prior to executing in production.
- Customer Preview testing – this is an opportunity for customers to gain early access to a future upgrade of the SAP Fieldglass application. This allows customers to gain confidence that the system is working as expected prior to the release date. Customer participation is optional.
- SAP Fieldglass regression testing – the SAP Fieldglass application is offered in a Software as a Service (SaaS) model. One of the services we provide is testing of the application prior to each production release. To ensure a customer's configuration, integrations, and reports are working as expected with the new codebase, SAP Fieldglass Quality Assurance uses a scrubbed production copy of the database in our regression testing. Regression testing is where we execute test cases against the current production codebase and the future codebase using a common data input. Output files from each test are compared to ensure any changes are expected.

Customers may opt out of this process. However, all responsibility in ensuring the customer's SAP Fieldglass instance is properly working and maintained is transferred to the customer.

To date, all SAP Fieldglass customers have declined to assume this responsibility.

1.6.5 Data Scrubbing

In order to properly service our customers, access to production data is required. All customer data is classified as Confidential. SAP Fieldglass takes every possible precaution to ensure data is protected from unauthorized access and misuse.

Data is protected in the following ways:

- First names and last names of buyers, suppliers, and workers are anonymized by replacing with a test value.
- Email addresses of buyers, suppliers, and workers are changed to a single false email address such as qatest8@SAP Fieldglass.com which is configured to automatically purge all email sent to it.
- Buyer and supplier company names are anonymized.
- Any custom fields created by the customer remain unchanged. Custom fields that contain sensitive data are encrypted with AES-256 and optionally display masked when entering and displaying values in the user interface. There is no way to decrypt these values since the decryption keys between production and test are different. Keys are stored in the corporate password vault and

access is limited to only select senior members of the technology team. This access list is reviewed quarterly by the internal audit team and by a third party in our annual SSAE 16 / ISAE 3402 Type 2 SOC1 and SOC2 audits.

The data scrubbing process is:

- A backup of the data is taken at the location where the source database resides
- Data is filtered where only the most recent 3 months of data remain
- Data is scrubbed as described above
- Data is then securely transferred from the production system to the test system

Once scrubbed, all personally identifiable information (PII) has been removed and any sensitive custom field data cannot be read.

Our test systems reside in secure third party data centers with the same controls as our production data centers.

1.6.6 Data Access

Direct access to production data is required in specific cases. Access is provided based on business need and not by role alone. Access reviews are conducted monthly and reviews are subject to recurring quarterly reviews by the SAP Fieldglass internal audit team. Executive review and sign off is performed for all quarterly reviews.

Access is required for the following puposes:

- Professional Services Data Services team – this team receives a customer's master and/or worker data and executes data uploads into test and/or production environments. Once the data are successfully uploaded and customer has signed off on the accuracy and completeness of the upload, the data are destroyed.
- First level help desk – when customers call our help desk, the caller may require the help desk agent to to view data or log in as the caller in order to help them with their problem. This is only performed when authorized by the caller.

SAP Fieldglass has help desk locations in the following regions:

United States

SAP Fieldglass
111 N. Canal Street
Suite 600
Chicago, IL 60606

Europe and APAC

Merlin-IT Hungary Information Technology Services Kft. Vagohid u. 2., 4034 Debrecen, Hungary	Merlin Information Systems Philippines Inc. 6th Floor C ommerce and Industry Plaza Building, McKinley Hill Cyberpark, Taguig City, Philippines

The SAP Fieldglass Security team conducted an onsite security audit in 2014 at Merlin Hungary. Contractually, Merlin must meet SAP Fieldglass' security requirements. The following security controls are in place:

- Help desk agents are not able to cut/paste using their secured workstation.
- External media including any USB drive is disabled.
- Printing is not supported.
- Help desk agents have been background checked by Merlin using SAP Fieldglass' background check requirements (see section 1.4.7 Background Checks).

1.6.7 Data Loss Prevention

Our DLP solution has been installed and configured for use on devices subject to exposure to sensitive information. It has been implemented to guard data at its endpoints and to ensure leakage of information classified as Confidential does not occur. Policies can be pushed from the central management console or pulled from an individual endpoint client. Client installs are configured to update (pull) policy changes every 90 minutes.

Our enterprise SIEM tool is configured to pull data in real time from the DLP database. Dashboards are created to allow quick overviews of agent statuses/details, alert details, and logging details.

The SIEM is configured to notify the Security Team in real time when an alert is detected. The Analyst then logs into the SIEM and investigates the alert to determine whether it's legitimate or a false positive.

1.6.8 Customer Termination

If a customer were to terminate their contract with SAP Fieldglass, the customer's data could be sliced out of the production database and delivered to the customer on a media of their choice. The size of the data will determine what media is appropriate.

2 Release Management

2.1 Release Management Process

The SAP Fieldglass Release Management team is responsible for the management of all delivables required in upgrading the production SAP Fieldglass system. This team is comprised of key members from the Development, Quality Assurance, Product Management, Professional Services, and executive teams. SAP Fieldglass customers benefit from our release management in that the release deployment schedule repeats itself year over year; releases are deployed over the same weekends of predetermined months.

SAP Fieldglass has several different release types:

Major Releases

In the US, Major releases occur on the second Fridays in March, July, and November. In the EU, Major releases occur on the third Fridays in March, July, and November

These releases can include new product features, new or changed functionality, user experience enhacements, and changes to the user interface. These are our most formal releases and the only type of release that requires an extended maintenance window. The Release Manager and the Release Management team closely monitor all phases of the Software Development Lifecycle and analyze PKIs at each phase transition. Release notes are provided as well as an opportunity for customers to optionally participate in a customer preview opportunity. This is where users can log into a non-production environment that is running the future codebase. The benefit of participating is that customers can gain confidence the system is behaving as expected prior to the official release date.

Minor Releases

Minor releases occur on the second Fridays in January, May and September.

These releases do not require the formalities of major releases. This type of release is used when deploying customer-specific product features and integrations to production. These releases are deployed to both US and EU customers at the same time.

Service Packs

Serivce packs are deployed as required to resolve product defects. These releases are deployed to both US and EU customers at the same time.

All releases are deployed to production by a central deployment team located in the US. During the deployment process, the codebase is replaced with the new codebase and data transformation scripts are executed. During this process, customer data is not viewed or accessed. Upon completion of the deploy, the Quality Assurance team executes a post-deploy verification checklist to ensure the system is ready for general availability. One such verification is verifying an MD5 hash to ensure the certified codebase was installed in production without modification. Test companies are used in conducting all testing.

3 Disaster Recovery and Business Continuity Plan

3.1 Disaster Recovery

SAP Fieldglass maintains a disaster recovery plan with backup, hardware repair, and data restoration, along with the ability to bring up the SAP Fieldglass application at a hot backup site in the event of a declared disaster (as described in the SAP Fieldglass disaster recovery plan) where the primary site is destroyed or disabled. This plan is tested on a yearly basis. Lessons learned are recorded in the test results and the plan is adjusted and improved accordingly.

SAP Fieldglass has the concept of active and passive production hosting facilities. The active environment is the live production hosted facility that all SAP Fieldglass users are actively using. The passive environment is a hot production hosting environment. Our data replication solution ensures that the passive environment is ready at anytime to be failed over to. In a disaster scenario, SAP Fieldglass changes the DNS to the passive hosting center's set of IPs. Users are then seamlessly routed to the other datacenter. There is not multi-day data migration that has to occur due to the ongoing data replication that is in place.

SAP Fieldglass proactively conducted a datacenter failover from the active datacenter to the passive datacenter in April 2015. The entire failover process was conducted in just over 8 hours with zero data loss. SAP Fieldglass plans to repeat this proactive datacenter failover between 1 and 3 times per year.

Also refer to section 1.6.1 Data Backups and Replication.

3.2 Business Continuity

The primary objective of our business continuity plan (BCP) is to enable SAP Fieldglass to recover all functions within their respective Recovery Time Objectives (RTOs) after any type of disruption occurs which prevents SAP Fieldglass personnel from engaging in ongoing business operations. A Recovery Point Objective (RPOs) has also been defined to identify our tolerance for any data loss. This Plan is designed to support the employees responsible for leading recovery efforts to enable SAP Fieldglass to resume daily operations following a disruption.

A business impact analysis (BIA) has been developed to fully quantify and prioritize restoration of mission-critical processes.

Privacy Policies and Procedures

Revision History

Virtru's Privacy Policies and Procedures were adopted as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Table of Contents

- Revision History
- Company
  - Document Control
  - Security Document Library
- Management and Protection of Personally-Identifiable Information
  - Overview:
  - Purpose:
  - Applicability:
  - Definitions:
  - Policy:
  - Enforcement:
- Administrative Requirements for HIPAA Implementation
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Documentation Requirements:
  - Enforcement:
- Minimum Necessary Standard
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Procedures:
  - Enforcement:
- Business Associate Agreements
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Enforcement:
- Business Associate Subcontractor Agreements
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Enforcement:
- Receipt, Use and Disclosure of Personally-Identifiable Information
  - Overview:
  - Purpose:
  - Applicability:
  - Special Definition:
  - Policy:
  - Procedures:
  - Enforcement:
- Complaint Process

- Overview:
- Purpose:
- Applicability:
- Policy:
- Procedures:
- Enforcement:

Scanner and Fax Policy
- Overview:
- Purpose:
- Applicability:
- Special Definitions
- Corporate Policies:
- Procedure:
- Enforcement:

Scanner Policy
- Overview:
- Purpose:
- Applicability:
- Special Definitions
- Corporate Policies:
- Procedure:
- Enforcement:

Training Policy
- Overview:
- Purpose:
- Applicability:
- Policy:
- Enforcement:

I. Company

Virtru may be referred to as "**Company**."

A. Document Control

A staff copy of this document is available with the **Virtru** Privacy Officer, Will Ackerly, willackerly@virtru.com or (202) 577-3683.

B. Security Document Library

These policies and procedures and related privacy and security practice information will be kept in our Security Documentation Library (SDL). The Library is located in Google Drive and backed up to a local NAS.

Outdated and superseded materials from the Security Documentation Library (or Notebook) will be kept in an archive (the Security Documentation Archive) for at six (6) years after the date when they are first outdated or superseded.

II. Management and Protection of Personally-Identifiable Information

A. Overview

The Privacy Rules place certain restrictions on the acquisition, use and disclosure of Personally-Identifiable Information (PII). These policies establish the minimum care with which PII in the custody of **Virtru** personnel must be maintained.

B. Purpose

The purpose of this document is to provide basic instruction to all **Virtru** employees regarding the management and protection of Personally-Identifiable Information.

C. Applicability

This policy applies to all **Virtru** employees, which are defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru.**

D. Definitions

Covered Entity means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Personally-Identifiable Information (PII) means any information about an individual maintained by **Virtru,** including:

1. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Treatment, Payment and Health Care Operations (TPO) include all the following:

1. *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
2. *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
3. *Health Care Operations* includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of healthcare professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities including the creation of de-identified health information as defined by these regulations.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

Employees means all employees of **Virtru** as well as its temporary employees, interns, independent contractors, trainees, and other persons in the performance of work for the **Company**, its offices, programs or facilities.

Privacy Rules means the rules adopted by various state and federal agencies to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated under this Act as well as those obligations that arise under the privacy and security standards adopted by the Health Insurance Marketplaces, pursuant to 45 C.F.R. §155.260.

E. Policy

For details on specific requirements, refer to the appropriate policies in this manual as indicated in *[brackets]*.

1. Generally: Personally-Identifiable Information shall not be obtained, used or disclosed except as permitted or required by law.

2. Permitted and Required Uses and Disclosures: Personally-Identifiable Information may or shall be disclosed as follows:

   a) To the individual

   b) To carry out TPO activities as allowed under HIPAA and/or pursuant to and in compliance with a current and valid Authorization *[Receipt, Use and Disclosure of Personally-Identifiable Information].*

   c) In keeping with a Business Associate Agreement *[Business Associate Agreement].*

   d) As otherwise allowed or required under the HIPAA Rules or other federal and/or state laws concerning privacy of information that is used by **Virtru** in the course of its business operations.

3. Minimum Necessary: Generally, when obtaining, using or disclosing Personally-Identifiable Information, or when requesting PII from another entity, reasonable efforts must be made to limit the PII used or disclosed to the minimum necessary to accomplish the intended purpose. However, the Privacy rules were not intended to severely complicate business processes and **Virtru** may, where appropriate, use a single format to provide data containing PII for our various services *[Minimum Necessary Standard].*

4. De-identified Personally-Identifiable Information: PII may be considered not to be individually identifiable in the following circumstances:

   a) The following identifiers of the individual (and relatives, employers or household members) are removed. (This is the "Safe Harbor" method that **Virtru** will generally use.)

      - Names
      - Information relating to the individual's geographic subdivision if it contains fewer than 20,000 people
      - Elements of dates (except year) directly related to the individual
      - All ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older
      - Telephone numbers
      - Fax numbers

- Email addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers; full face photographic images
- Any other unique identifying number, characteristic or code.

b) As allowed in the Privacy Rules, **Virtru** shall provide a number of longitudinal identifiers in the de-identified data. These identifiers shall not allow identification of the individual who is the subject of this data in that:
    1) These identifiers will be encrypted using industry level encryption techniques
    2) The method of encryption shall not be divulged to the receiver of the de-identified data

5. Complaint Process: **Virtru** has put into place a process for individuals to make complaints about our Privacy Policies and Procedures and/or our compliance with those Policies and Procedures.

6. Documentation: **Virtru** must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of six (6) years from the later of the date of creation or the last effective date.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies. *[Sanction Policy]*

III. Administrative Requirements for HIPAA Implementation

A. Overview

The Privacy Rules require that a Business Associate have in place appropriate administrative safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions regarding **Virtru**'s obligations relating to the implementation of administrative requirements of the Privacy Rules.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

1. Personnel Designations: **Virtru** has designated and documented designations of the following:
   a. Will Ackerly has been designated as the Privacy Officer.
      1) He is responsible for the development and implementation of corporate-wide policies and procedures relating to the safeguarding of Personally-Identifiable Information.
      2) He will also be responsible for receiving complaints relating to Personally-Identifiable Information and for providing information about the **Company's** privacy practices.

   b. Persons with access to Personally-Identifiable Information are listed by title and department including a listing of individuals' names on the Risk Assessment; and will be updated if **Virtru** makes any major changes to processes, staff, programming or company location; or at a minimum annually. **Virtru** will retain the previous listing for a period of not less than six (6) years.

2. Training Requirements: **Virtru** shall document the following training actions: All **Virtru** employees shall receive training on applicable policies and procedures relating to Personally-Identifiable Information as necessary and appropriate for such persons to carry out their functions within the **Company**.

   a. Each new employee shall receive the training as described above within 30 days after joining **Virtru**.

b. Each employee whose functions are impacted by a material change in the policies and procedures relating to Personally-Identifiable Information, or by a change in position or job description, shall receive the training as described above within 30 days after the change becomes effective.

c. Complaints handled by Committee...

3. Safeguards: **Virtru** shall have in place appropriate Administrative, Technical, and Physical Safeguards to reasonably safeguard Personally-Identifiable Information from intentional or unintentional unauthorized receipt, use or disclosure.

4. Complaint process: **Virtru** shall have in place a process for individuals to make complaints about the **Company**'s HIPAA Policies and Procedures and/or **Virtru**'s compliance with those Policies and Procedures, and shall document all complaints received and the disposition of each complaint. (See Complaint Process)

5. Sanctions**:** Our Privacy Policies call for our workforce that has access to Personally-Identifiable Information to perform certain duties and to refrain from certain actions. Failure to do so will be sanctioned according to the policy below.

These sanctions apply to the designated workforce members including managers, supervisors, and staff who have access to Personally-Identifiable Information.
It is intended as guidance for our business management in sanctioning information security policy infractions. We reserve the right to implement sanctions differently if, in our judgment, the situation warrants it.

We define a serious infraction as one that results in known significant damage or that threatens imminent significant damage. Other infractions are simple infractions.

First security infraction

If the infraction is:

a. A simple infraction, and
b. The first infraction in the last 3 years

The sanction will be retraining the workforce member on the appropriate policy/procedure and placement of a written letter of reprimand in the employee file. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Second security infraction or first serious infraction

If the infraction is:

a. A serious infraction, or

b. The second infraction of either type within 3 years

The sanction will include a written letter of reprimand that is given to the person at fault, placement of a copy of the letter in the employee file, and one week's suspension without pay. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Third security infraction or second serious infraction

If the infraction is:

a. A second serious infraction within 3 years, or
b. A third infraction of any type within 3 years.

The sanction will be dismissal from the workforce.

Virtru makes exceptions for disclosures made by employees who qualify as whistleblowers or certain crime victims.

6. Mitigation efforts required*:* **Virtru**, to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclosures of Personally-Identifiable Information by the **Company** or any of its Business Associate Subcontractors.

7. Prohibition on intimidating or retaliatory acts: Neither **Virtru** nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of Personally-Identifiable Information in violation of the regulations.

Virtru shall document the following actions relating to its policies and procedures:

a. Required policies and procedures: **Virtru** shall implement policies and procedures to assure appropriate safeguarding of Personally-Identifiable Information in its operations.
b. Changes to policies and procedures: **Virtru** shall change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. **Virtru** may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, **Virtru** shall make correlative changes in its Privacy Notice.

E. Documentation Requirements

Virtru must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the Privacy Rules, for a period of six (6) years from the later of the date of creation or the last effective date.

F. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

IV. Minimum Necessary Standard

A. Overview

The Privacy Rules place certain restrictions on the receipt, use and disclosure of Personally-Identifiable Information in regards to the amount reasonably necessary to accomplish the task being performed. However, the Privacy Rules also allow Personally-Identifiable Information to be disclosed for business appropriate needs.

The policies developed by **Virtru** will follow this business appropriate philosophy as well as that of administrative simplification, which is the subsection of the HIPAA law under which the Privacy Rule was developed. **Virtru** shall use standard data formats for information acquisition or disclosure and tailor these formats to contain a business reasonable minimum necessary amount of Personally-Identifiable Information. The **Company's** policies establish the minimum necessary use provisions for Personally-Identifiable Information in the custody of **Virtru** employees.

B. Purpose

To issue instructions regarding **Virtru's** obligations relating to the Privacy Rules to obtain, use and disclose only the minimum amount of Personally-Identifiable Information (PHI) necessary to accomplish the intended purpose.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of the **Company**.

D. Policy

Virtru will make reasonable efforts to ensure that the Minimum Necessary amount of Personally-Identifiable Information is disclosed, used, or requested to accomplish the intended purpose. Exceptions to the Minimum Necessary Standard include disclosures:

1. To the individual who is the subject of the information;

2. Made pursuant to an authorization provided by the individual;
3. To healthcare providers for treatment purposes;
4. Required for compliance with the standardized HIPAA transactions;
5. Made to the Secretary of HHS or his agent pursuant to a privacy investigation;
6. Otherwise required by the Privacy Rules or other law.

Employees shall be trained on the policies and procedures developed to apply these principles to the use or disclosure of, or requests for Personally-Identifiable Information.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

1. Each user of a system which accesses Personally-Identifiable Information shall be identified and the classes or types of PII to which access is needed and any conditions appropriate to such access will be established. It will be the responsibility of the Privacy Officer to maintain this information using the *Employee Access Request Form* [**Forms for Employees**] and *System Access Log* [**Change Control Logs for Security**].

2. Reasonable efforts will be taken to limit the access of each user of Personally-Identifiable Information to the amount needed to carry out the individual's duties. These efforts will include internal use of PII.

3. For situations where Personally-Identifiable Information disclosure occurs on a routine and recurring basis, the PII disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the disclosure.

4. Requests for disclosures that are not routine and recurring and thereby covered by **Virtru** standard procedures (other than to the individual, the Secretary of HHS or his agent, or where required by law) shall be reviewed by the Privacy Officer to determine that the Minimum Necessary Standard is applied to the extent reasonable.

5. Questions regarding these procedures should be directed to the **Virtru** Privacy Officer, Will Ackerly, willackerly@virtru.com, or (202) 577-3683.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

V. Business Associate Agreements

A. Overview

The Privacy Rules impose certain requirements on Business Associates who create, receive, use or disclose Personally-Identifiable Information on behalf of their Covered Entity partners. **Vitru** must comply with the requirements in this section.

B. Purpose

To provide instructions to all **Virtru** employees regarding the necessity of and the requirements for Business Associate Agreements relating to Covered Entities.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru.**

D. Policy

1. Generally: A Covered Entity may disclose Personally-Identifiable Information to **Virtru**, or allow **Virtru** to create or receive PII on the Covered Entity's behalf. **Virtru** will appropriately safeguard the PII obtained from the Covered Entity. **Virtru** will document these assurances through a written agreement.

2. Content Requirements: The agreement between the Covered Entity and **Virtru** must meet the following requirements, as applicable:

    a. Establish permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized for the Covered Entity, except that the agreement may permit **Virtru** to use or disclose Personally-Identifiable Information for its own management and administration if such use or disclosure is required by law, or **Virtru** provides reasonable assurance to the Covered Entity to which the Personally-Identifiable Information is disclosed that the confidentiality of the PII will be maintained.

    b. Provide that **Virtru** will:

        1. Not use or disclose the Personally-Identifiable Information except as authorized under the agreement or required by law.
        2. Use safeguards to prevent unauthorized use or disclosure.
        3. Report unauthorized uses or disclosures to the Covered Entity.

4. Pass on the same obligations relating to protection of Personally-Identifiable Information to any subcontractors.
5. Make Personally-Identifiable Information available for access by the Covered Entity in accordance with relevant law and policy.
6. Make Personally-Identifiable Information available to the Covered Entity for amendment, and incorporate any approved amendments to Personally-Identifiable Information, in accordance with relevant law and policy.
7. Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
8. Make its internal practices, books and records relating to its receipt or creation of Personally-Identifiable Information available to the Secretary of HHS for purposes of determining **Virtru's** compliance with Privacy Rules.
9. Authorize termination of the agreement by the Covered Entity upon a material breach by **Virtru**.

3. Compliance Responsibilities: Virtru agrees to report any use or disclosure of Personally-Identifiable Information not permitted by this agreement and any successful security incident to Covered Entity within a commercially reasonable period, but in no event later than within thirty (30) business days, after it is discovered.

E. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use of Personally-Identifiable Information was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

VI. Business Associate Subcontractor Agreements

A. Overview

The Privacy Rules impose certain requirements on Business Associate Subcontractors who create, receive, use or disclose Personally-Identifiable Information on behalf of **Virtru**. All Business Associate Subcontractors of **Virtru** must comply with the requirements in this section.

B. Purpose

To provide instructions to all **Virtru** employees regarding the necessity of and the requirements for Business Associate Subcontractor Agreements relating to Business Associate Subcontractors who receive, use or disclosure Personally-Identifiable Information on behalf of **Virtru**.

C. Applicability

This policy applies to all **Virtru** employees and Business Associate Subcontractors, which are defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru** and the Business Associate Subcontractor.

D. Policy

1. Generally: **Virtru** may disclose Personally-Identifiable Information to a Business Associate Subcontractor, or allow a Business Associate Subcontractor to create or receive PII on **Virtru**'s behalf, if adequate assurances are obtained by **Virtru** that the Business Associate Subcontractor will appropriately safeguard the PII. **Virtru** must document these assurances through a written agreement. This requirement does not apply with respect to:
   a. Disclosures made to a provider concerning the individual's treatment, payment or health care operations; or
   b. Uses or disclosures made to a governmental agency for purposes of public benefit eligibility or enrollment determinations where such company is authorized by law to make these determinations.

2. Content Requirements: The agreement between **Virtru** and a Business Associate Subcontractor must meet the following requirements, as applicable:

   a. Establish permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized for the entity, except that the agreement may permit the Business Associate Subcontractor to use or disclose Personally-Identifiable Information for its own management and administration if such use, or disclosure is required by law, or the Business Associate Subcontractor obtains reasonable assurance from the entity to which the Personally-Identifiable Information is disclosed that the confidentiality of the PII will be maintained.

   b. Provide that the Business Associate Subcontractor will:
      1) Not use or disclose the Personally-Identifiable Information except as authorized under the agreement or required by law.
      2) Use safeguards to prevent unauthorized use or disclosure.
      3) Report unauthorized uses or disclosures to **Virtru**.
      4) Pass on the same obligations relating to protection of Personally-Identifiable Information to any subcontractors or agents.
      5) Make Personally-Identifiable Information available for access by **Virtru**, in accordance with relevant law and policy.

6) Make Personally-Identifiable Information available to **Virtru** for amendment, and incorporate any approved amendments to PII, in accordance with relevant law and policy.
7) Make information available to **Virtru** for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
8) Make its internal practices, books and records relating to its receipt or creation of Personally-Identifiable Information available to the Secretary of HHS for purposes of determining the Business Associate Subcontractor's compliance with Privacy Rules.
9) If feasible, return or destroy all Personally-Identifiable Information upon termination of contract; if any PII is retained, continue to extend the full protections specified herein as long as the PII is maintained.
10) Authorize termination of the agreement by the entity upon a material breach by the Business Associate Subcontractor.

3. Compliance Responsibilities: If **Virtru** knows of a pattern or practice of the Business Associate Subcontractor that amounts to a material violation of the Agreement, **Virtru** and the Business Associate Subcontractor must attempt to cure the breach to end the violation, and if unsuccessful, terminate the agreement. If terminating the Agreement is not feasible, **Virtru** must report the problem to the Secretary of HHS.

E. Enforcement

An employee of **Virtru** or an employee of the Business Associate Subcontractor found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use of Personally-Identifiable Information was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

VII. Receipt, Use and Disclosure of Personally-Identifiable Information

A. Overview

The Privacy Rules impose certain requirements on Covered Entities and Business Associates who create, receive, use or disclose Personally-Identifiable Information on behalf of their Covered Entity partners.

B. Purpose

To provide instructions to all **Virtru** employees regarding the receipt, uses and disclosures of Personally-Identifiable Information, which are permitted or required by HIPAA.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of the **Company**.

D. Special Definition

Public Health Authority means a governmental company or authority, or a person or entity acting under a grant of authority from or a contract with such a public company, including the employees or agents of the public company, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

E. Policy

State and federal law permit and require certain receipt, uses and disclosures of Personally-Identifiable Information such as those related to Business Associate Agreements. Additional uses and/or disclosures are allowed or required that related to public responsibility that require no agreement or authorization on the part of the individual who is the subject of the PII. It is the policy of **Virtru** to obtain, use and disclose PII only as permitted and/or required by law or regulation including the following situations:

1. Treatment, Payment or Healthcare Operations: Personally-Identifiable Information may be used or disclosed for the purposes of providing treatment, payment or healthcare operations. Such disclosures will be made only as allowed by and pursuant to prevailing state and federal law.
    a. Discussions involving Personally-Identifiable Information shall be conducted only in appropriate business areas including but not limited to offices, conference rooms and other non-public areas;
    b. Conducted only for the purpose of fulfilling a legitimate business need; and
    c. Conducted with regard to and in compliance with the "Minimum Necessary Standard." *[Minimum Necessary Standard]*

2. Contained in a Business Associate Agreement: For permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized by the Covered Entity in a Business Associate Agreement.

3. Required by Law: Personally-Identifiable Information may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.

4. Abuse and Neglect: Except for reports of child abuse or neglect, Personally-Identifiable Information about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law

enforcement activity. The individual whose Personally-Identifiable Information has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

5. Judicial Proceedings: Personally-Identifiable Information may be disclosed in response to a court order.

6. Law Enforcement: Personally-Identifiable Information may be disclosed for the following law enforcement purposes and under the specified conditions:
    a. Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries
    b. Decedent's Personally-Identifiable Information may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct
7. Serious Threats to Health or Safety: Consistent with applicable law and ethical standards, Personally-Identifiable Information may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and are not permitted when the information is learned in the course of treatment to affect the propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

8. Specialized Government Functions: National Security and Intelligence: Personally-Identifiable Information may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other activities authorized by the National Security Act.(45 CFR 164.512(k)(2))

9. Protective Services: Personally-Identifiable Information may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons. (45 CFR 164.512(k)(3));

10. Public Benefits: Personally-Identifiable Information relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

11. Workers' Compensation: Personally-Identifiable Information may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

F. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

Any request for disclosure of Personally-Identifiable Information, 1) pursuant to a court order, warrant or subpoena; 2) by a law enforcement agent; 3) by a public health authority; or 4) by a national security, intelligence or other federal company, must be directed to the Privacy Officer and the CEO for review and action. Any such request will include an acknowledgement of receipt to insure that the document was actually received by the appropriate corporate individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer and CEO.

G. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

VIII. Complaint Process

A. Overview

The Privacy Rules require that **Virtru** provide a process for individuals to make complaints concerning the **Company**'s policies and procedures required by these regulations and document all complaints received, and the dispositions of these complaints, if any.

B. Purpose

To issue instructions regarding **Virtru** obligations relating to the Privacy Rules to provide a process for individuals to complain about the **Company**'s policies and procedures and the requirement to document complaints received and the disposition of these complaints.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

Virtru shall maintain a process to receive complaints from individuals about **Company** Privacy Policies and Procedures, for complaints from individuals who believe their privacy rights have been violated and from employees or Business Associate Subcontractors who believe that **Virtru** is not abiding by its policies and procedures and/or assurances concerning Personally-Identifiable Information. This process shall include the following:

1. Any complaints or questions should be submitted to the Privacy Officer or his assistant.
2. All service and complaint issues will be stored in the Desk.com app.

Virtru shall work in good faith to resolve complaints received to the satisfaction of the submitter, where possible.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

1. Complaints shall be submitted in writing on paper or electronically.

2. Complaints shall be entered into the complaint tracking system either automatically or by the individual designated to provide information on the **Company** complaint process. and when manually entered shall be in the exact words provided by the submitter.

3. The **Virtru** Privacy Officer shall investigate complaints and make a determination as to whether or not the complaint has merit.

4. The **Virtru** Privacy Officer shall present complaints received to **Virtru**'s senior executive for immediate action.

5. If the Privacy Officer has completed the investigation of the complaint and made a determination, such determination shall be presented to the **Virtru** Executive Board

6. If the investigation has not been completed nor a provisional determination made by the Privacy Officer, it shall be the prerogative of the senior executive to make a summary determination or to direct the Privacy Officer to continue with the investigation and to report on the complaint at the next scheduled meeting.

If a determination is made that **Virtru** is in violation of the privacy provisions of the Privacy Rules or that changes are needed in the Privacy Policies or Business Associate Agreement to clarify the allowed practices of **Virtru**, the **Virtru** CEO and Privacy Officer shall determine the actions that the **Company** shall take.

Complaint determinations and actions that **Virtru** takes pursuant to such complaints, if any, shall be reported to the submitter of the complaint, if such person is known. Privacy Officer, or his designated agent, shall update the complaint tracking system with the findings of the Privacy Officer's investigation, any determination made, direction or actions of the **Virtru** CEO and Privacy Officer with regard to the complaint, and a copy of any information provided to the submitter in response to their complaint.

F. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

IX. Fax Policy

A. Overview

The Privacy Rules require that **Virtru** implement appropriate administrative, technical, and physical safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions to all **Virtru** employees regarding the use of faxes with respect to Personally-Identifiable Information and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to **Virtru** from damages, which may result from unauthorized disclosure of Personally-Identifiable Information through facsimile use.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Special Definitions

Fax: An electronic facsimile of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a fax machine, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Personally-Identifiable Information to people who do not have a need to know such information.

E. Corporate Policies

Employees must exercise utmost caution when sending faxes to parties outside of **Virtru**. Faxes containing Personally-Identifiable Information should only be received on and sent to user or departmental specific fax machines and not to systems that have general access.

In cases where Personally-Identifiable Information is received from outside on a non-departmental specific fax machine, the receiving department shall notify the **Virtru** Privacy Officer of the source of such information. The employee shall communicate the approved fax number to the external entity and record such actions. Should PHI be disclosed by fax to an inappropriate party, **Virtru** shall, to the extent possible, remediate such disclosures.

All fax documents sent by **Virtru** employees shall contain the following statement:

This fax is intended for the individual/individuals or entity/entities named above and may be covered by copyrights, business partner confidentiality agreements, non-disclosures or other legally binding instruments. If you are not the intended recipient, do not read, copy, use or disclose the contents of this communication to others. Immediately notify the sender by reply fax, destroy all hard copies and delete this document from all systems. Thank you!

F. Procedure

In the cases where data that contains Personally-Identifiable Information is disclosed by fax machine use to an inappropriate party, the following procedure shall be followed:

1. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the fax without reading.
2. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
3. A fax shall also be sent to the receiving party containing the same instructions as detailed for the phone call requesting a return fax message indicating that the requested action was taken.
4. The cause of the inappropriate disclosure shall be determined and reported to the **Virtru** Privacy Officer.

Methods to prevent a reoccurrence of the inappropriate disclosure shall be formulated and put into place.

Any additional actions prescribed by regulations shall be performed to the extent possible.

G. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use

or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

X. Scanner Policy

A. Overview

The Privacy Rules require that **Virtru** implement appropriate administrative, technical, and physical safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions to all **Virtru** employees regarding the use of scanners with respect to Personally-Identifiable Information and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to **Virtru** from damages, which may result from unauthorized disclosure of Personally-Identifiable Information.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Special Definitions

Scanner: An electronic copy of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a computer, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Personally-Identifiable Information to people who do not have a need to know such information.

E. Corporate Policies

Employees must exercise utmost caution when scanning and transmitting these documents to their devices and parties outside of **Virtru**. Scans containing Personally-Identifiable Information should only be received on and sent to user or departmental specific computer in an encrypted format, or sent using **Virtru's** encrypted email application.

F. Procedure

In the case where scanned data that contains Personally-Identifiable Information is disclosed to an inappropriate party, the following procedure shall be followed:

1. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the scan without reading.

2. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
3. The cause of the inappropriate disclosure shall be determined and reported to the **Virtru** Privacy Officer.

Methods to prevent a reoccurrence of the inappropriate disclosure shall be formulated and put into place. Any additional actions prescribed by regulations shall be performed to the extent possible.

G. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XI. Training Policy

A. Overview

The Privacy Rules require that **Virtru** train their employees on the requirements of our Privacy Policies and Procedures developed to protect the Personally-Identifiable Information to which employees are provided access. The **Company** has determined that all employees of **Virtru** shall be trained on Privacy so that we can provide the necessary assurances for the protection of Personally-Identifiable Information to our clients, vendors and business partners as required under the Privacy Rules.

B. Purpose:

To provide instructions to all **Virtru** employees regarding the requirement for HIPAA training.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

1. General: It is the policy of the **Company** that all employees of **Virtru** and its current and future subsidiaries be trained on Privacy and the **Company** policies and procedures created to protect Personally-Identifiable Information.

2. Duty Specific Training: Privacy training shall be appropriate to the tasks that each employee performs. In the case where an employee does not come into contact with Personally-Identifiable Information as a normal course of the employee's duties, the employee shall be trained on the corporate policies and procedures.

3. New Employees: New employees shall be trained on the corporate policies and procedures as part of their normal employment process and shall be trained on our Privacy Policies and Procedures, if applicable, within 30 days of being employed by **Virtru.** The Assistant ISO, Jordan Duggan, shall document this training and provide the Privacy Officer with documentation of this training within the 30-day period.

4. Transfers: When an employee transfers from one department to another, the employee shall be trained on our Privacy Policies and Procedures within 30 days of being assigned. Jordan Duggan shall document this training and provide the Privacy Officer with documentation of this training, within the 30-day period.

5. Material Change in Policies and Procedures: when a material change in the policies and procedures occurs, each employee shall receive training on such changes within 30 days of the implementation of the change. Jordan Duggan shall document this training and provide the Privacy Officer with documentation of this training, within the 30-day period.

E. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Security Policies and Procedures

{After choosing where you will store your Security Documents, delete either the **Library** or {Notebook} option throughout this document.}

Revision History

Virtru's Security Policies and Procedures were adopted as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Security Policies and Procedures

Table of Contents

- Virtru
  - Document control
  - B. Security Document Library
- II. Preface and Background Material
  - Overview
  - B. Policy
- III. Key Concepts
  - Information Security Principles
    - Confidentiality
    - Integrity
    - Availability
    - Provability
  - Definitions
    - Information Security Policy
    - Privacy Policy
    - Acceptable Use Policy for IT Systems Users
    - Employment Policies
- IV. Using These Standards
  - Audience – Who will use this document
    - Technology and business process providers should comply with these Standards as a matter of contractual obligation
    - Employees and Business units within Virtru should comply, unless a Risk Assessment has been done and a deviation is approved by the ISO
  - How the document is used
    - Review of existing controls, procedures and tools against the Standards
    - Documenting compliance or deviations
    - Gap Analysis to determine where improvements are needed
    - A Risk Assessment to validate that the improvements are justified against the costs of the controls and the value of the information involved
    - Creation of a plan to close the gaps OR signoff of a deviation
    - Documentation of the new controls, procedures and tools
  - C. Maintaining this document
- V. Roles and Responsibilities
  - A. Rules for ownership of information
  - B. Information users
  - C. Information Security Officer
    - Manage awareness programs relating to security and privacy topics
    - Maintain a central record of exceptions to this Standards document
    - Manage changes to this Standards document

Security Policies and Procedures

Provide leadership relating to new security risks, controls and technologies
Oversee and approve the sharing and reuse of Personal Identifiable Information (PII) collected by or processed by the company
VI. Information Classifications and Requirements
Overview
B. The Security classification process
IT platforms such as servers and workstations
IT applications including database transaction processing and email
Data sets
Paper copies of information
Information types typically known to workforce members, such as customer information
Development, acquisition or deployment of software
Connections of computers or networks to outside systems or networks
Granting of access to any outside organizations
C. The classes of information for Security and Privacy
Data Types
Company-owned data that relates to such areas as corporate financials, employment records, payroll, etc.
Setting requirements for business continuity
Required uptime for the information asset
Required restoration time if the data must be restored
Required frequency of backups
Requirements for storage of backups
Requirements for testing of the recovery process
Enforcement
VII. Handling Rules for the Information Classifications
Overview
Inventory of Information Assets and Electronic Asset Management Log
Rules for access to information assets
VIII. Access Control Policy
Overview
Access levels
Granting access
The ISO will provide accounts with the matching technical privileges and give the workforce member the account information including a one-time-use password that the user must change to a private password upon first use of the account.
1. Only the person assigned to an account will be allowed to use that account.
Vendors, contractors and other outsiders
Individuals
Policy

Security Policies and Procedures

IX. Rules by Data Classification
- Public/unclassified data
- B. Private/internal data
- C. Confidential or protected data
- D. Managing data sources
- E. Retention of media
  - Agent of Record letters and Letters of Authorization requests are held for no less than ninety (90) days
  - New Business Group documents are held for no less than ninety (90) days
  - General documents are held for no less than ninety (90) days
  - Banking statements are held for seven (7) years
  - Workforce member records are held for seven (7) years
- F. Sanitization of Media
- G. Information sharing and privacy
- H. Release of company information

X. Risk Analysis and Management
- Risk reviews
- B. Risk management
  - Increasing a protection to a level higher than what is listed in this document
  - Improving oversight or monitoring of the risk to limit impact and minimize response time
  - Limiting transactions or other events to minimize the possible impact of the risk event

XI. IDs and Accounts
- User IDs
- B. ID and account creation
  - Expiration dates for the User ID
  - Renewal process for the User ID
  - Documentation of the role, business process and job function relating to the User ID
- C. Account management
- Application Specific IDs

XII. Authentication and Passwords
- Overview
- Password format
- Rules

XIII. Authorization and Rights Management
- General Access Roles
  - Super Admin Access: Access to all front and backend products as well as product metrics
  - Admin Access: Access to all front end products as well as product metrics
  - General Access: Access to product metrics

- Low Access: Access to corporate email, sales, and marketing data only
- Amazon Web Services (AWS)
- Cloudant
- Github
- ELK Stack
- Mixpanel
- Kissmetrics
- Salesforce

Access Rules

- Limiting access to datasets and types
- Limiting access to operating systems
- Limiting times of access

Temporary Privileged Users and Accounts

D. Assignment and Revocation Procedure

- An Employee Access Log for all new hires and/or workforce member change of status.
- An Exit Checklist for all terminations.

E. Logout After Inactivity

XIV. Breaches or Impermissible Uses/Disclosures

Definitions

- Penetrations of systems, applications, networks or databases
- Denial of service attacks
- Misuse or mishandling of assets
- Virus or other malware contamination
- Transaction errors
- Breaches of confidentiality agreements or contracts
- Legal or regulatory violations

XV. Breach Response

A. Overview

Confidential Reporting:

- Calling (may leave voice message) the ISO or AISO
- Sending an email to the ISO or AISO, or;

XVI. Personnel Security

Screening for newly hired personnel, third parties, vendors

- Professional qualifications
- Identity checks
- Criminal checks
- Confirmation of academic and professional experience

B. Training and Awareness

- Managing malicious software (e.g. viruses)
- Using workstation(s) securely

- Managing passwords and
- Monitoring and reporting suspicious use of account(s)
- C. Terms of employment
- D. Acknowledgement
- E. Exit process for users
  - Relinquish all access to control devices
  - Report all User IDs in use by the person
  - Relinquish all information stored, whether on paper or on backup media
  - Relinquish all information processing devices, including workstations, all
  - Virtru-owned mobile devices and others
  - All systems access will be revoked.
- Security Sanction Policy
  - First Security Infraction
    - A simple infraction, and
    - The first infraction in the last 3 years
  - Second Security Infraction or First Serious Infraction
    - A serious infraction, or
    - The second infraction of either type within 3 years
  - Third Security Infraction or Second Serious Infraction
    - A second serious infraction within 3 years, or
    - A third infraction of any type within 3 years
    - The sanction will be dismissal from the workforce.

XVII. Legal and Regulatory Issues
- Legal processes
- Copyrights and licenses
- C. Export controls

XVIII. Malware and Antivirus
- Definitions
- Operating system anti-malware requirements
  - Macintosh, Linux and iPhones:
  - PC Operating Systems:
  - Android and Windows Phone Operating Systems:
- Affiliates
- Infected devices
- Employees' Requirements
  - Workforce members will not load software on our Company's information equipment without permission from the ISO.
  - Workforce members will not open electronic files from unfamiliar sources.
- Enforcement

XIX. Change Control Logs
- Preface

Security Policies and Procedures

- B. Policy
  - Sufficient information is available for proper investigation of use, misuse, incidents and performance
  - User ID, event type, date and time are maintained
  - Time is according to a known time stamp so that events across systems can be coordinated
  - 4. End-to-end accountability is always maintained
  - Changes to operating systems, application code or other tools
  - Backup and restore events
  - Changes affecting any cryptographic keys or devices
  - Stop or start of critical processes
  - Transaction failure, retry or duplication
  - KissMetrics
  - Segment.io
  - Sendgrid
- XX. Encryption
  - Preface
  - Application Encryption Policy
  - Key Rotation Policy
  - D. Device Encryption Policy
    - Mac OS Devices:
    - Windows OS Devices:
    - Linux OS Devices
    - Android Devices
    - Windows Phone
    - iPhone
  - E. Wi-Fi network encryption
  - F. Email encryption
  - G. Enforcement
- XXI. Assessments and Testing
  - Overview
  - B. Penetration testing
    - Operating systems
    - Applications
    - Databases
  - C. Vulnerability assessment testing
    - A new system, application or network is installed inside the Company
    - Changes are made to firewalls, VPNs or other security control tools
    - Changes are made to a web server's operating system
    - Changes are made to email servers
    - Configuration changes are made to databases

Configuration changes are made to critical applications
Changes are made to encryption scheme(s)
D. Wireless access testing
E. Password testing
XXII. Use of Email, Internet, Messaging, Public Sites, Blogs, Social Media
Policy
Sexually explicit material
Confidential, Private or Protected Information or Internal Use material, except as meets the Handling Rules section
Viruses
Threats
Inappropriate or unlawful language, including:
Offensive language
Language inappropriate for the Company environment
Discriminatory or harassing language
Tools usable for hacking, password cracking, vulnerability scanning or penetration testing
XXIII. Hardware
Definitions
B. Policy
C. Asset management
D. Enforcement
XXIV. Networks
Overview
Denial of service attacks
Improper access
Virus infections
Unauthorized software installations, email, FTP or other improper usage
Administration of network and communications connections
Operations of all devices
Monitoring
Timely review of audit logs and response to alerts or alarms
Review of unusual patterns of usage or activity
Monitoring
Access control and physical security
Access limited to authorized personnel only
Physical security, including RFID or passcode controlled locks, are in place
Modifications, updates
Documentation
Network design
Segmentation

- Firewalls
- Internet
  - Approved by the ISO
  - Periodically reviewed and tested for vulnerabilities
  - Protected by firewalls, intrusion detection systems and anti-malware tools
- VPN-remote access
- Wireless
- Telework Policy
- Patching of systems and applications
- Network hardening

XXV. Physical and Environmental Protections

- Definitions
  - Computing centers
  - Network connection points
  - Media storage locations
  - Locations containing platforms which carry high-value or critical information or transactions
- B. Secure Sites Policy
  - Media libraries
  - Electrical supplies and controls
  - Environmental and mechanical controls

XXVI. Physical Security Policy

- A. Entry Policy
- Loss of RFID key
- Mobile devices
- D. Video monitoring
- Alarm system
- Fire protection

XXVII. Software

- Overview
- B. Acquisition of software
- C. Open Source Software
  - It is not used in a production environment OR
  - Prior to use it is fully tested, documented and Virtru's personnel are assigned to support it. Checks to be performed include:
  - The source of the software is documented
  - URL
  - Project lead
  - Contributors
  - The ISO approves of the use
- D. Documentation

- E. Change control and maintenance
- F. Operating Systems
- G. Applications
  - Access control
  - Authorization
  - Information classification
  - Storage controls
  - Backup and restoration
  - Confidentiality and integrity requirements
  - Audit logs
  - Privacy, export control and other such requirements
- H. Asset management for software
- I. Enforcement

XXVIII. Removable Media Device Policy
- Purpose
- B. Scope
- C. Definitions
- D. Policy
- E. Using Removable Media Devices
- F. Exceptions
- G. Refusal
- H. Enforcement

Application Recovery Plan
- Overview
- Scope
- Data durability and reliability
- Encryption
- Load balancing
- Restoration of data
- G. Testing and revision of plan

Network Attached Storage and Workstation Backup Plan
- Overview
- Policy
- Backup software
- Remote backups
- Local backups
- Encryption of backups
- Restoring data
- H. Enforcement

Information Integrity Management Policy
- Overview

Security Policies and Procedures

B. Policy
Security Incident Management Policy
Overview
Procedures
C. Policy
Security Plan Review Policy
Overview
Procedures
Appendices
Change Logs
B. Information Security Committee

Security Policies and Procedures

I. Virtru

Virtru may be referred to as "**Company**."

A. Document control

A staff copy of this document is available with the Information Security Officer (ISO), Will Ackerly, willackerly@virtru.com (202) 577-3683, and Assistant Information Security Officer(AISO), Jordan Duggan, jordan@virtru.com (202) 577-3683.

B. Security Document Library

These policies and procedures and related security practice information will be kept in our **Security Documentation Library** (SDL). The **SDL** is located in google drive and backup to the Synology NAS.

Documentation about security practices (logs of activities, etc.) will either be kept in this SDL (or Notebook) or in a short file in the SDL that will describe where the security practice documentation resides. The intended result is that anyone with access to the SDL will be able to locate any piece of documentation associated with our security program.

Outdated and superseded materials from the SDL will be kept in an archive (the Security Documentation Archive) for at least seven (7) years after the date when they are first outdated or superseded.

II. Preface and Background Material

A. Overview

It is vital to the reputation and profitability of **Virtru** that our information and our clients' information, in all forms, be protected from unauthorized use, modification, loss, copying, etc. This document sets out the default standards, which must be met to ensure that control.

Our information may exist on paper, in voice systems, on IT systems and networks, in the minds of our people, and in other forms. The information which needs protection includes, but is not limited to:

1. Client information (both for customer companies and for people as individuals)
2. Financial information, including credit cards, salaries, banking, transactions and more
3. Medical information of all types
4. **Company** patents, business plans and other intellectual property

5. **Company** business records and planning materials, including our customer list, marketing and sales efforts, product line plans and more
6. Copyrighted materials, both which our **Company** creates and those which we obtain under license from others

B. Policy

Compliance with these standards is mandatory. Any deviation from these standards must be approved beforehand by the ISO.

III. Key Concepts

A. Information Security Principles

The protection of information can be described in several key dimensions:

1. Confidentiality
2. Integrity
3. Availability
4. Provability

In this document, the standards given are the **Company** defaults. They must be applied where appropriate, but always balanced against the cost of implementing the control, and the value of the information involved.

B. Definitions

To prevent confusion, these are the definitions used throughout this document.

Policies: Corporate documents which set out **Virtru's** position regarding business processes, behavior of personnel and similar topics. Policies are a high-level statement of **Virtru's** position. Some of **Virtru's** policies, which relate to information security are:

1. Information Security Policy
2. Privacy Policy
3. Acceptable Use Policy for IT Systems Users
4. Employment Policies

Standards: Rules that must be followed to enable an effective information security program. Compliance with the Standards is mandatory, but deviation is possible if approved by the ISO.

Standards define the minimum baseline procedures, practices and configurations for systems, applications, controls, networks and related topics. Standards are designed to provide a single reference point for use during software development and adoption,

installation of systems and tools, and during the contracts process with vendors and service providers. Standards do not, however, give detailed command-line instructions on how to meet the **Virtru's** policies. Those are given in the guidelines.

Guidelines: Built for each application and platform; to be followed when implementing that particular tool. A Guideline may vary a bit from one implementation to another, as long as the Security Standards are met and justification is given and properly documented.

Combined, these three levels of documents provide a method for **Virtru** to audit itself and ensure proper controls are in place, without excess cost or risk. They also provide a means for **Virtru** to explain to regulators, examiners, external auditors or investors how our **Company** is safe, trustworthy and efficient.

IV. Using These Standards

A. Audience – Who will use this document

This document applies to **Virtru's** employees, business units and any Business Associate Subcontractor supporting **Virtru**:

1. Technology and business process providers should comply with these Standards as a matter of contractual obligation
2. Employees and Business units within Virtru should comply, unless a Risk Assessment has been done and a deviation is approved by the ISO

B. How the document is used

This Standards document is a reference point to ensure a consistent framework of protections is in place. Implementing these standards involves:

1. Review of existing controls, procedures and tools against the Standards
2. Documenting compliance or deviations
3. Gap Analysis to determine where improvements are needed
4. A Risk Assessment to validate that the improvements are justified against the costs of the controls and the value of the information involved
5. Creation of a plan to close the gaps OR signoff of a deviation
6. Documentation of the new controls, procedures and tools

No signoff or approvals are needed if a level of protection higher than what is given in this Standard is determined to be needed for a given information asset.

C. Maintaining this document

This document must be reviewed at least once a year or anytime there are significant changes in software or security. Updates must be made to keep it in accord with **Virtru's** overall business goals and risk position. The document will be reviewed by the ISO or AISO. Any updates, improvements or suggestions should be sent to the ISO.

V. Roles and Responsibilities

A. Rules for ownership of information

The information and systems provided by **Virtru** to workforce members, contractors and representatives are owned by **Virtru**, which also determines appropriate usage and access rules. All data on **Virtru's** systems and networks is owned by **Virtru**, with the exception of software that the ISO has approved to be open sourced or otherwise transferred to another entity through code escrow or code exchange and/or trade.

In this document, the words 'information owner' refer to the person who owns the responsibility for the information. The information itself remains the property of **Virtru**.

B. Information users

Every user of **Virtru's** information must protect that information and ensure that it is used for **Virtru's** business purposes only. Any incidents or questionable issues in the security of our information must be reported to the ISO or AISO.

Information users may not assign access rights, authorize destruction or copying of information, or change the protections given to information assets. Information users must comply with all laws, regulations and **Virtru's** policies and procedures.

C. Information Security Officer

Virtru's ISO and AISO will:

1. Manage awareness programs relating to security and privacy topics
2. Maintain a central record of exceptions to this Standards document
3. Manage changes to this Standards document
4. Provide leadership relating to new security risks, controls and technologies
5. Oversee and approve the sharing and reuse of Personal Identifiable Information (PII) collected by or processed by the company

See Appendices for further information and *Information Security Committee* for a current listing of members.

VI. Information Classifications and Requirements

A. Overview

Information is classified by system to ensure that the controls applied to it are sufficient and also to ensure that the controls applied do not impair **Virtru's** business, ability to compete or **Virtru's** image.

All information must have a classification for security and must have requirements set for business continuity.

B. The Security classification process

Each information asset will go through the following classification process. Information assets include, but are not limited to:

1. IT platforms such as servers and workstations
2. IT applications including database transaction processing and email
3. Data sets
4. Paper copies of information
5. Information types typically known to workforce members, such as customer information

In general, an information asset includes both the raw information itself (paper, oral or data entry), the location where it resides, the business processes which handle it and the systems and tools that handle it.

Information assets will also be reviewed during:

1. Development, acquisition or deployment of software
2. Connections of computers or networks to outside systems or networks
3. Granting of access to any outside organizations

The security classification of an information asset is assigned according to the highest of these dimensions. As an example, if an asset is regulated by law, then it needs the highest classification, even if the asset is not critical to the Company's business.

C. The classes of information for Security and Privacy

This policy applies to all workforce members, management, contractors, vendors, business partners and any other parties who have access to Company or client data.

Data Types

The security classification of an information asset is assigned according to the highest of these dimensions. As an example, if an asset is regulated by law, then it needs the highest classification, even if the asset is not critical to **Virtru's** business. **Virtru** deals with two main kinds of data:

1. **Company-owned data** that relates to such areas as corporate financials, employment records, payroll, etc.

2. **Personally Identifiable Information (PII)** that is the property of our clients or workforce members, such as Protected Health Information, social security numbers, credit card information, contact information, etc.

D. Setting requirements for business continuity

The requirements for an information asset relating to business continuity are not set by classification, but are specific to that asset. They include:

1. Required uptime for the information asset
2. Required restoration time if the data must be restored
3. Required frequency of backups
4. Requirements for storage of backups
5. Requirements for testing of the recovery process

The default requirements for business continuity are listed in the information handling rules' section. See *Handling rules for the information classifications* in this document and *Disaster Recovery Plan* for detailed information.

This section outlines the basic rules for handling information types according to the classifications. More specific standards for platforms, processes and networks appear in each topic section of this standards document.

E. Enforcement

It is the responsibility of everyone who works at **Virtru** to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

VII. Handling Rules for the Information Classifications

A. Overview

This section outlines the basic rules for handling information types according to the classifications. More specific standards for platforms, processes and networks appear in each topic section of this standards document.

B. Inventory of Information Assets and Electronic Asset Management Log

An inventory is maintained of all significant information assets belonging to, or used by **Virtru**. This inventory includes:

1. Serial numbers/license numbers
2. MAC Addresses
3. Model
4. Device Type
5. Manufacturer
6. The information owner
7. Username
8. Location
9. OS Version
10. The custodian of the information and repository location (database, file cabinet, etc.)
11. Purpose in our systems
12. Asset value in dollars or other suitable measurement
13. The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
14. Requirements for the asset regarding availability, uptime, etc.
15. Contact information for one or more parties who can repair, restore, replace, or recover this asset. Examples are hardware/software vendors, IT support vendors, and/or staff members

This asset list contains information that is restricted to executives and super-admins, and therefore is stored securely on the Synology NAS, which itself is backed up to AWS Glacier.

This inventory will be reviewed and updated quarterly, or as new assets and devices are added. Logs are maintained as the *Inventory of Information Assets Log* and the

Organizational Chart/Electronic Asset Management Log. A current copy of this inventory will be kept at a separate location as described in our *Disaster Recovery Plan.*

C. Rules for access to information assets

If any given security incident involves a breach of Personally Identifiable Information (PII), the ISO will follow our security policies and *Incident and Breach Policy* for handling such a breach.

If a security incident includes the potential that personal information may have been obtained by unauthorized individuals, the ISO will work with the client to notify affected persons of this event, in compliance with relevant federal and/or state law.

See also *Breaches or Impermissible Uses/Disclosures* within these Security Policies and Procedures.

VIII. Access Control Policy

A. Overview

This policy defines how **Virtru** manages access to electronic information and systems. **Virtru** provides access to electronic data relative to the workforce member's job requirement. We limit access to categories of data and systems that each person needs to do his/her job. We require that each workforce member restrict his/her access to only those specific records and functions needed to carry out his/her job. For the purposes of this policy workforce members are anyone in **Virtru** who has access to Personally Identifiable Information (PII).

B. Access levels

The ISO will qualify the workforce member to have one of these forms of access based on the job role (in order of increasing access permissiveness):

1. Low Access to Corporate Email and Salesforce Data
2. General Access to product metrics
3. Admin Access to all front end products as well as product metrics
4. Super Admin Access to all front and backend products as well as product metrics

The access will match the person's job responsibilities The ISO will keep a record of the type of access provided to each workforce member. The record will include a date and justification and will be kept in our *Employee Access Request Log* in the **Security Documentation Library.**

The granting of access to Business Associate Subcontractors will be done in the same way as it is done for workforce members.

C. Granting access

The ISO will provide accounts with the matching technical privileges and give the workforce member the account information including a one-time-use password that the user must change to a private password upon first use of the account.

1. Only the person assigned to an account will be allowed to use that account.

2. Each time a user logs in to a system, a log will be maintained by that specific program with the following information
    a) When the user accessed the system
    b) What information the user accessed while in the program
    c) Tracking will be done by using the User ID and IP Address
    d) The ISO will maintain this log for a period of 1 year

3. The ISO and AISO will each have a special account that allows them to create new accounts. The accounts will be used:
    a) In an emergency when all other accounts have been disabled or locked out;
    b) To either reset the passwords on locked accounts; or
    c) To create new accounts that provide needed access.

4. When a change in the role of a workforce member requires a change in access privileges, the ISO will reassess the needs and provide new access privileges based on the policy in Access Levels in this section.
    a) If a workforce member leaves **Virtru**, the ISO will remove that member's access as soon as the access is no longer needed.
    b) If a workforce member takes a leave of absence and is not expected to require access, the ISO will disable the workforce member's account when he/she leaves and re-enable it upon his/her return to work.
    c) For other people who work around protected electronic information but are not qualified to access it, the ISO will decide which of the following two steps to take:
        1) Train the person to understand his/her responsibilities
        2) Supervise while he/she is exposed to the data
    d) For cases in which the provision of individual accounts is not feasible {e.g. access by any one person of a large help desk staff of a vendor}, the ISO will make:
        1) A serially reusable account and provide a one-time-use password to the vendor's representative for each time that access is needed; and

2) The password will be changed by the ISO on the account after each use of the account to a value not known to the vendor.

D. Vendors, contractors and other outsiders

Any outside organization that wishes to gain access to our or our client's Private/Internal, Confidential or Protected information must:

1. Sign a Business Associate Subcontractor Agreement; AND
2. Be willing and able to show that their privacy and security controls are at least as stringent as **Virtru's** controls.

See *Business Associate Subcontractor Agreement* for details of Agreement.

A written history of incidents reported by Business Associate Subcontractors (BAS) will be maintained. If the ISO becomes aware of a pattern of activity in which the BAS is not carrying out the contractually required safeguards, then the ISO will do one of the following:

1. Attempt to remedy this failure
2. Terminate the contract, if attempt to remedy is not feasible
3. Report the situation to the U.S. Secretary of Health and Human Services, if terminating the contract is not feasible.

If any given security incident involves a breach of Personally Identifiable Information, the ISO will follow our privacy policies and incident management plan for handling such a breach.

If a security incident reported by a BAS includes the potential that personal information may have been obtained by unauthorized individuals, the ISO will work with the BAS to notify affected persons of this event in compliance with relevant federal and/or state law.

See also *Breaches or Impermissible Uses/Disclosures* within these Security Policies and Procedures.

E. Individuals

Individual persons who work for such an organization must also be bound to the outside organization's controls. Such individuals must:

1. Have Business Associates Subcontractor Agreement with their own company; OR
2. Have a contract with their company; AND
3. Have appropriate background checks and bonding in place.

F. Policy

Virtru will not knowingly accept any confidential information belonging to third parties until that information is reviewed against our protections and the appropriate agreements put into place and signed by the information owner. The agreements should include all requirements for controls over the third-party information and the processes to be followed.

IX. Rules by Data Classification

A. Public/unclassified data

This type of information does not require special marking or storage, except to ensure that it is available when needed. It does need to be kept safe from unauthorized modification.

B. Private/internal data

Access is granted on a need-to-know basis, as authorized by the manager of the user of the information. Some types of jobs are automatically granted access to data in this class.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes:

1. Printing this class of information only to a known printers located in secure areas on secure networks.
2. Encrypting or physically securing backup media
3. Keeping paper copies of information locked or otherwise secured

This class of information is not released to anyone outside **Virtru** without a non-disclosure agreement, a Business Associate Subcontractor Agreement, and/or without the approval of the information owner. Private/Internal use information must not be transmitted across any unsecured outside network or path without proper controls. This means encryption for files and emails or secured packaging for paper copies.

C. Confidential or protected data

Access to this type of information is on a need-to-know basis, as approved by the ISO or information owner.

This class of information is not released to anyone outside the Company without a non-disclosure agreement and without the approval of the information owner.

Confidential or Protected information must not be transmitted across any unsecured outside network or path without proper controls. This means encryption for files and emails, or secured packaging for paper copies.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes:

1. Printing this class of information only to a known, secure printer
2. Encrypting and physically securing backup media
3. Keeping paper copies of information locked or otherwise secured

D. Managing data sources

The key to managing **Virtru's** business' media and documents is to first consider the source of the information, then the media type. **Virtru's** media and documents containing Protected Information (PHI, CJIS, or other) require protection from inception through disposition. Regardless of the owner relationship, the Company will be cognizant of the following Media Types:

1. **Hard Copy:** paper printouts, printer and facsimile ribbons, drums, etc.
2. **Electronic:** the bits and bytes contained on hard drives, flash drives, phones and tablets.

E. Retention of media

Retention: The length of time documentation and/or information is retained according to the level of confidentiality and to the business continuity requirements. System/ information owners should consult with the ISO to ensure compliance with the record retention regulations.

Virtru's hard copy record retention policy is as follows:
We will digitize and encrypt these records for secure storage on the Synology NAS, which will be backed up to AWS Glacier.

Virtru's electronic record retention policy is as follows:

1. Agent of Record letters and Letters of Authorization requests are held for no less than ninety (90) days
2. New Business Group documents are held for no less than ninety (90) days
3. General documents are held for no less than ninety (90) days
4. Banking statements are held for seven (7) years
5. Workforce member records are held for seven (7) years

F. Sanitization of Media

When media (hard copy and electronic) becomes obsolete, is no longer required or no longer usable, it is critical that proper sanitization is accomplished.

Sanitization Types

Disposal: the act of discarding media. This is often done via recycling paper containing "non-confidential" material.

*Reinitializing***:** Re-formatting drives so information cannot be retrieved by recovery utilities or any other forms including keystroke recovery attempts. This is achieved by overwriting the disk with zeros for no less than one (1) time.

Purging: exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains, this is also known as degaussing.

Destroying: destruction of media so it cannot be reused as its original purpose.

Virtru's electronic disposal policy is as follows:

1. Hard-drives are purged, reinitialize or destroyed
2. CD or DVD disks are destroyed
3. Flash drives are re-initialized or destroyed
4. Backup tapes are purged, reinitialized or destroyed

Any systems that are leased must be securely sanitized of all Company data prior to being returned to the leasing company. Any additional media (e.g. hard drives, USB drives etc.) will be reformatted then written with zeros for no less than one (1) time to ensure that the data contained on the media has been destroyed.

Virtru shall maintain appropriate records of sanitization. This entails validating how, where and when media is sanitized. See *Media Sanitization*.

G. Information sharing and privacy

In most cases the sharing and reuse of Personally Identifiable Information is governed by law, regulation and customer expectation. To ensure **Virtru** meets those requirements, no Personally Identifiable Information will be shared with outside companies, vendors or personnel without written approval from the ISO.

Personally Identifiable Information includes:

1. Names
2. Addresses

3. Phone Numbers
4. Email Address
5. Dates of birth
6. Social Security Numbers
7. Ages
8. Gender
9. Personal Financial Information
10. Personal Medical Information
11. Criminal History Information
12. Personal Employment Information
13. Personal Buying Histories
14. IP Addresses

Aggregated and statistical data developed from this personal information is not personally identifiable and, thus, does not need the approval of the ISO for sharing and re-use.

Virtru will comply with all applicable laws and regulations regarding the privacy of personal information, including such laws as:

1. Health Insurance and Portability and Accountability Act (HIPAA)
2. Health Information Technology for Economic and Clinical Health (HITECH)
3. Family Educational Rights and Privacy Act (FERPA)
4. Criminal Justice Information Systems (CJIS)
5. Federal Information Security Management Act (FISMA)

Virtru's workforce members, contractors, vendors and suppliers may come into possession of Personally Identifiable Information as a part of their relationship with **Virtru**. Each person must comply with all laws, regulations and policies and ensure such information is properly protected.

H. Release of company information

Virtru's information may only be released with the approval of the ISO or the information owner. This includes the posting of **Virtru's** information of any type onto bulletin board systems, public networks, social media or other open sharing tools. Any information released must contain proper copyright, trademark, disclaimer and patent notices as appropriate.

X. Risk Analysis and Management

Risks to **Virtru's** assets and environment should be addressed proactively rather than reactively. The controls applied to the risks must also be periodically reviewed to ensure the controls are working properly and efficiently.

Security Policies and Procedures

A. Risk reviews

The job of reviewing risks and setting requirements for controls is the ISO's. Risks should be reviewed or assessed when:

1. Developing or deploying new applications, systems, networks or software
2. When significant changes are made to that same list
3. When business processes change
4. When **Virtru** enters a new geographical area of business
5. When **Virtru** enters a new line of business
6. When incidents occur or new risks emerge
7. When new regulations or standards are set

B. Risk management

Risks may be accepted, avoided or mitigated.

Accepting the risk is appropriate when the cost of avoiding or mitigating the risk is greater than the expected loss. The losses considered should include the less tangible items such as **Virtru's** reputation, loss of market share and loss of public trust in **Virtru**. Acceptance of a risk requires complete documentation of the risk analysis and approval by the information owner.

Avoiding the risk is appropriate when the cost of insurance is less than the cost of incremental controls. However, basic controls must always be in place.

Mitigating the risk is appropriate in most situations. These situations are those where compensating controls are possible, cost-effective and manageable. These mitigating controls may include:

1. Increasing a protection to a level higher than what is listed in this document
2. Improving oversight or monitoring of the risk to limit impact and minimize response time
3. Limiting transactions or other events to minimize the possible impact of the risk event

The method chosen for managing the risk (acceptance, avoidance, mitigation) must match the business value and costs involved and must be approved by the information owner.

For further detail, see the *Risk Management Policy* and the *Disaster Recovery Plan*.

XI. IDs and Accounts

A. User IDs

Each user shall be assigned a unique identification, called the User ID. This User ID is not considered to be sensitive, unless the User ID relates to an authentication process, systems or application management role.

On sensitive systems or applications the User ID should not be easily identifiable, thus making unauthorized usage more difficult.

Sharing of User IDs is not permitted, unless justified by business requirements and approved by the ISO. For any such shared User ID, the password will be shared using LastPass, and the password will not be shared with the additional user. If this password is shared, it must be changed immediately after the User ID is used to keep the shared User ID from becoming generally available and a risk to **Virtru**.

Guest and anonymous User IDs are not allowed, unless the system involved is not connected to any of **Virtru's** networks and the system does not have any **Company** information on it. Typically, these guest or anonymous User IDs are only used during development or during marketing/sales demonstrations.

B. ID and account creation

User IDs are only to be created following a process approved by the information owner. This User ID creation process should include:

1. Expiration dates for the User ID
2. Renewal process for the User ID
3. Documentation of the role, business process and job function relating to the User ID

User IDs are to be created for the purpose needed and not in a manner to compromise segregation of duties.

A record of all User IDs and their owners will be maintained by the ISO. See the **Change Control Logs for Security** for further detail.

C. Account management

A periodic check will be made of all User IDs and any redundant, dormant or unused IDs will be removed. The ISO must review the privileges set up for User IDs no less than once every year.

D. Application Specific IDs

Application Specific IDs and logins are used in support of automated applications, transactions, processes or batch jobs. These have non-expiring passwords.

1. Application Specific IDs must not be used by individuals.
2. Application Specific IDs must be created only with the approval of the ISO, must be documented and have strictly limited access rights.
3. Application Specific IDs must not have ad hoc or interactive capabilities on the applications, systems, transactions or data involved.

XII. Authentication and Passwords

A. Overview

All systems, applications, databases or other information repositories shall require users to authenticate themselves prior to granting access. Authentication may be via an approved password scheme or via an access control device. All systems that support 2-factor authentication must have them enabled.

The authentication method used must suit the value of the information asset, matching the cost of the authentication method against the level of protection required. In general, administrative and other high-value User or Service IDs will use the most secure methods of authentication.

B. Password format

Must be at least twenty (20) characters in length and must contain characters from all of the following four (4) categories:

1. English uppercase characters (A through Z)
2. English lowercase characters (a through z)
3. Base 10 digits (0 through 9)
4. Non-alphabetic characters (for example, ! , @, #, $)

C. Rules

Users are forced to create a new password every 3 months. Users must not write down on paper or store any passwords; they must also never share their passwords with other users. Software is provided to securely store user passwords, with encryption.

A maximum 5 attempts will be permitted prior to disabling the account. New passwords must be different from the previous three (3) passwords. Passwords must be changed immediately upon first use of a new ID. Passwords must never be stored or transmitted in clear text. Systems must not echo back the password as it is entered.

Passwords must not be retained by any system or application longer than is needed to grant access. Initial passwords must be transmitted separately from the ID.

XIII. Authorization and Rights Management

A. General Access Roles

Access roles are defined as:

1. *Super Admin Access:* Access to all front and backend products as well as product metrics
2. *Admin Access:* Access to all front end products as well as product metrics
3. *General Access:* Access to product metrics
4. *Low Access:* Access to corporate email, sales, and marketing data only

Amazon Web Services (AWS)
Users who have access to AWS have Super Admin Access. User sessions will expire after one (1) hour of inactivity

Cloudant
Users who have access to Cloudant have Super Admin Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Github
Users who have access to Github have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

ELK Stack
Users who have access to ELK Stack have Admin Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Mixpanel
Users who have access to Mixpanel have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Kissmetrics
Users who have access to Kissmetrics have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Salesforce
Users who have access to Salesforce have General Access. User sessions automatically time out after twenty (20) minutes.

Segment.io
Users who have access to Segment.io have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

B. Access Rules

User IDs and accounts must be authorized to access only those elements needed for the user's role, including:

1. Limiting access to datasets and types
2. Limiting access to operating systems
3. Limiting times of access

Access to operating systems, ad hoc transaction capabilities, software development tools, and other system devices must be controlled and limited to only those User IDs which require that access.

Segregation of duties shall be established for all information asset controls to minimize the possibility that one person is responsible for an entire asset.

A user (and hence User ID) that changes role or job function must have access rights updated to match the new job role or function. Any changes will be documented in the *Responsibility Change Log*.

C. Temporary Privileged Users and Accounts

Temporary privileged users are defined as those who:

1. Have any control over security tools on an application, system or network
2. Can update operating systems or similar tools
3. Can directly modify data within a database or application
4. Have any special capabilities built in by the vendor of the application software, operating system or platform

Access at a temporary privileged user level shall be granted only on a need-to-know, need-to-perform basis, and then only to the assets required. Temporary privileged user access shall only be granted to those supporting **Virtru's** applications, networks and systems.

D. Assignment and Revocation Procedure

The ISO shall electronically complete:

1. An Employee *Access Log* for all new hires and/or workforce member change of status.
2. An *Exit Checklist* for all terminations.

E. Logout After Inactivity

The ISO shall verify that all users have activated a password-protected screensaver that automatically prevents unauthorized users from viewing or accessing electronic protected information from any system or device that can be used to access electronic information systems. After a maximum of 10 minutes of inactivity the system should log off and lock the device, making information inaccessible. Once logged off a user must re-enter a password to gain access to electronic protected information.

XIV. Breaches or Impermissible Uses/Disclosures

A. Definitions

Incident is defined as any breach of security, privacy, continuity, legal or regulatory controls over information assets of any type. Examples of such incidents include but are not limited to:

1. Penetrations of systems, applications, networks or databases
2. Denial of service attacks
3. Misuse or mishandling of assets
4. Virus or other malware contamination
5. Transaction errors
6. Breaches of confidentiality agreements or contracts
7. Legal or regulatory violations

Breach is defined as an impermissible access, use or disclosure, which compromises the privacy or security of PHI.

XV. Breach Response

A. Overview

Virtru will maintain an effective method so that all information users, custodians and owners can readily report incidents.

Incidents will be reported to the person's immediate manager or the ISO. Once the ISO has been notified, said Officer will then follow the directions in the *Incident and Breach Policy*.

The ISO will investigate incidents and will log or report significant losses or threats immediately. The appropriate authorities will be contacted by the ISO depending on the severity of incident.

Incidents involving misuse by workforce members will be investigated by the ISO.

Depending on the severity of the incident, the Emergency Contact list may provide additional contacts. See the *Emergency Contact List* located in the *Disaster Recovery Plan*.

Confidential Reporting:

Confidential reporting may be done either by:

1. Calling (may leave voice message) the ISO or AISO
2. Sending an email to the ISO or AISO, or;
3. Google Form for anonymous reporting

XVI. Personnel Security

A. Screening for newly hired personnel, third parties, vendors

Proper verification checks must be made prior to granting any new workforce member, contractor, vendor, agent or affiliate access to Private, Internal, Confidential or Protected information. These verification checks will meet the requirements set forth by the **Company** and may include:

1. Professional qualifications
2. Identity checks
3. Criminal checks
4. Confirmation of academic and professional experience

The ISO is responsible for ensuring that background checks are made biannually on parties who are not newly hired workforce members. A third party will conduct background checks.

B. Training and Awareness

Virtru will provide security awareness training to each new member of our workforce with access to electronic **Company**-owned or private data (Refer to Data Types information Classifications) whose activities in the business we directly control. The training will be provided prior to that person assuming his/her duties. The training is designed to inform the person of his/her responsibilities under **Virtru's** security policies. At a minimum, this training will include the workforce member's role in:

1. Managing malicious software (e.g. viruses)
2. Using workstation(s) securely
3. Managing passwords and
4. Monitoring and reporting suspicious use of account(s)

Virtru's employees will also be trained annually on **Virtru's** Policies and Procedures. A record of successful completion of this training and annual retraining will be kept online by **Total HIPAA Compliance**.

Within 30 days of starting, individuals who are employed as developers will receive training on the security measures and mechanisms used to protect the company's systems and service. All new developers will be required to take and pass online training modules covering secure coding when using Node.js. Developers who will be managing or developing operational aspects of the company's systems will also be required take the Security Operations on AWS training course from Amazon.

A record of training will be kept of training that lists the employee, type of training, date of completion, the employee's signature, and an admins signature asserting successful completion of the training.

C. Terms of employment

Compliance with **Virtru's** policies regarding security and privacy are a condition of employment.

D. Acknowledgement

All users shall be required to sign an acknowledgement after being trained on **Virtru's** security and privacy policies.

E. Exit process for users

Upon exiting employment or any relationship with **Virtru**, all users who have been granted access to any information asset shall:

1. Relinquish all access to control devices
2. Report all User IDs in use by the person
3. Relinquish all information stored, whether on paper or on backup media
4. Relinquish all information processing devices, including workstations, all **Virtru**-owned mobile devices and others

All systems access will be revoked.

The ISO will verify termination is completed, and document this procedure has been followed. See *Exit Checklist*.

F. Security Sanction Policy

Virtru's security policies call for the workforce that has access to electronic Protected Employee or Client Data and others to perform certain duties and to refrain from certain actions. Failure to do so will be sanctioned according to the policy below.

If the infraction involves the unauthorized use or disclosure of electronic Protected Employee or Client Data, the sanctions below apply to the designated workforce members including managers, supervisors, and staff who have access to Protected Employee or Client Data.

We define a serious infraction as one that results in known significant damage or that threatens imminent significant damage. Other infractions are simple infractions. The process below is intended as guidance for our business management in sanctioning Security Policies and Procedure infractions. We reserve the right to implement sanctions differently if, in our judgment, the situation warrants it.

First Security Infraction

If the infraction is:

1. A simple infraction, and
2. The first infraction in the last 3 years

The sanction will be retraining the workforce member on the appropriate policy/procedure and placement of a written letter of reprimand in the employee file.

The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Second Security Infraction or First Serious Infraction
If the infraction is:

1. A serious infraction, or
2. The second infraction of either type within 3 years

The sanction will include a written letter of reprimand that is given to the person at fault, placement of a copy of the letter in the employee file, and one week's suspension without pay. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Third Security Infraction or Second Serious Infraction
If the infraction is:

1. A second serious infraction within 3 years, or
2. A third infraction of any type within 3 years

The sanction will be dismissal from the workforce.

XVII. Legal and Regulatory Issues

A. Legal processes

Responses to subpoenas, deposition requests and other legal issues will be referred to and handled by the CEO. The ISO will not respond to such legal processes without company legal counsel.

B. Copyrights and licenses

Virtru may have agreements in place governing the use and handling of software, information and other tools that are owned by other entities. All users and information owners will comply with those agreements.

Users are responsible for complying with copyrights regarding any material obtained via the Internet. This includes files, graphics, software, audio and video materials.

Users may not agree to a new copyright license, unless given permission by the ISO.

Licensed software must be used in accordance with the license agreement and only the number of copies licensed must be created or used.

C. Export controls

Information may not be exported across country boundaries without prior written approval of the **Company**'s ISO.

XVIII. Malware and Antivirus

A. Definitions

Anti-Malware: malicious software that may reside on a computer, steal information or cause destruction. This can include a virus, trojan horse, keylogger, hijacker or dialer.

Sandbox: A highly controlled area where programs and software can be tested before being allowed access to the rest of the system.

B. Operating system anti-malware requirements

Macintosh, Linux and iPhones:
Virtru has determined that software for anti-malware scanning on Macintosh, Linux and iPhones is not necessary due to the low probability of encountering malware, the demand on computer processing power, and loss of productivity by the user. This policy will be reviewed annually or as needed to determine if this is still valid.

PC Operating Systems:
Data entering **Virtru's** Window-based systems must be subject to an up-to-date anti-malware scanning tool that is scheduled to run at regular intervals. In addition, all emails, attachments, disks, backup media, USB memory devices and other data carrying tools must be scanned before they are downloaded or allowed access to the system. All incoming data must be sandboxed by the anti-malware program before it is allowed access to the system. The anti-malware pattern files must be regularly updated.

Android and Windows Phone Operating Systems:
All such devices must have anti-malware tools in place prior to being connected to **Virtru's** networks. These systems must be subject to an up-to-date anti-malware scanning tool that is scheduled to run at regular intervals. In addition, all emails, attachments, and SD cards must be scanned before they are downloaded or allowed access to the system.

C. Affiliates

Virtru and all of its affiliates, contractors, consultants, vendors, representatives or other service providers must make certain that adequate controls are in place to guarantee that data coming from their systems and networks is free from malware.

D. Infected devices

The ISO will use approved tools to monitor and remove malicious software from **Virtru's** assets. Virus-infected computers, tablets or phones must be removed from the network immediately until they are verified as virus-free.

E. Employees' Requirements

1. Workforce members will not load software on our **Company's** information equipment without permission from the ISO.
2. Workforce members will not open electronic files from unfamiliar sources.
3. Will exercise best practices when using the **Virtru** network. The employee will not:
    a. Circumvent user authentication on any device
    b. Sniff network traffic
    c. Access data, servers, or accounts they are not authorized to access
    d. Cause a disruption of servers
    e. Violate copyright law by transmitting copyrighted pictures, music, video and/or software
    f. Export or import software, technical information, encryption software, or technology in violation of international or regional export control laws
    g. Use the Internet or network in a manner that violates **Virtru's** Security Policies, or local laws
    h. Intentionally introducing malicious code; including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers

The workforce will be trained to know and carry out these malware protections. The ISO will generally provide permissions as required above only for actions that are intended for our **Company's** business and only under conditions that limit the potential for the introduction of malware.

F. Enforcement

Any activities with the intention to create and/or distribute malicious programs into **Virtru's** networks (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.) are prohibited, and user will be subject to **Virtru's** Sanction Policy, and will be reported to the proper state and federal authorities.

XIX. Change Control Logs

A. Preface

The ISO is required to maintain logs of systems that document any changes and access users may have to sensitive systems. The following are the retention policies for these logs.

B. Policy

Audit logs will be retained for at least one (1) year in raw format, preferably electronic, to preserve evidence. Audit logs must be configured to prevent overflow, erasure or tampering. Audit logs will be configured to record information such that:

1. Sufficient information is available for proper investigation of use, misuse, incidents and performance
2. User ID, event type, date and time are maintained
3. Time is according to a known time stamp so that events across systems can be coordinated
4. End-to-end accountability is always maintained

Events to be recorded include, but are not limited to:

1. Login and activity by any other privileged accounts
2. Changes to operating systems, application code or other tools
3. Backup and restore events
4. Changes affecting any cryptographic keys or devices
5. Stop or start of critical processes
6. Transaction failure, retry or duplication

All systems and tools involved in the protection process are required to always have change logs enabled and properly configured. This includes:

1. Firewalls
2. Email servers
3. Anti-malware tools especially the administration tools
4. Security administration tools such as password resets and account modifications
5. Monitoring tools
6. Routers and other network devices
7. Github
8. Amazon Web Servers (AWS)

9. IBM Cloudant
10. SalesForce
11. Elk Stack
12. Mixpanel
13. KissMetrics
14. Segment.io
15. Sendgrid
16. Customer.io

Logs will be reviewed and analyzed by delegates of the ISO.

Reports of problems and incidents will follow the incident reporting method, listed in the *Incident and Breach Policy*.

XX. Encryption

A. Preface

Encryption is the process of encoding messages of information is such a way that only authorized parties can read it.

B. Application Encryption Policy

Virtru encrypts all client data using NIST-approved cryptographic modules. **Virtru** uses AES 256 encryption for its application. **Virtru's** key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the ISO.

C. Key Rotation Policy

Virtru requires the following key rotation policy to protect all external systems. The following is the list of policies for the following keys:

1. **Secure Socket Layer (SSL)Keys**
   Virtru uses SSL keys to enable Transport Layer Security (TLS) traffic between clients and **Virtru's** servers.

   Rotation Policy

Rotation of SSL Keys is done upon SSL Key expiration. They are set to expire at 1 (one) year and rotated at that time. If there is an incident or the security keys are thought to be compromised, the keys will be rotated immediately.

2. **Secure Shell (SSH) Keys**
   The SSH keys provide a layer of authentication to get into the production servers. SSH Keys are used as the authentication mechanism to remotely login to a server. They are also used as the first factor of authentication to assume root access on the production servers. Each developer has his/her own SSH key and is responsible for keeping this key secure.

   Rotation Policy
   All SSH keys are rotated at a minimum of every three (3) months. If there is an incident or the SSH keys are thought to be compromised, keys will be rotated immediately.

3. **Amazon Web Services (AWS) Access Keys**
   Unique AWS Access Keys are given to each developer with a unique AWS Login. This allows the developer to make Application Protocol Interface (API) calls to AWS. Currently, 1-2 AWS Access keys exist per developer. Where are these stored? How do you know how many keys each developer has?

   Rotation Policy
   These keys are rotated at a minimum of every 90 days. If there is an incident or the AWS keys are thought to be compromised, keys will be rotated immediately

4. **Application Keys**
   Virtru uses these keys to encrypt sensitive key data stored in the CouchDB database managed by IBM. There is only one copy of this key.

   Rotation Policy
   No rotation requirement.

   Backup Policy
   Backup of the key is kept with **Virtru's** Super Administrators.

The export of encryption technologies is restricted by the U.S. government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

D. Device Encryption Policy

Virtru requires devices have encryption enabled for any files, folders, drives, databases, or other stored data that may have sensitive information including protected personally identifiable information.

The implementation of any encryption scheme is performed by the user and the deployment of the encryption tool, including all keys, must meet industry best practices and be properly documented. Currently the minimum standard is 128-Bit encryption. Encryption keys will be managed by the user and a log will be maintained by the ISO.

Mac OS Devices:
Mac OS devices that store Protected Information (PHI, CJIS, etc), are required to use full disk encryption using FileVault 2. Users must provide a copy of their key to the ISO; both will maintain the key in a secure location.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Windows OS Devices:
Windows OS devices that store Protected Information (PHI, CJIS, etc) are required to use full disk encryption with the program Bitlocker. The encryption key will be maintained in a secure location by both the user and the ISO.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Linux OS Devices
Linux OS devices that store Protected Information (PHI, CJIS, etc) are required to use full disk encryption. This will be encrypted at a minimum of 128 bit encryption. The encryption key will be maintained in a secure location by both the user and the ISO.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Android Devices
All Android devices that store Protected Information (PHI, CJIS, etc) will have encryption turned on and will be password protected at all times. The encryption key will be maintained in a secure location by both the user and the ISO.

Windows Phone
All Windows Phones that store Protected Information (PHI, CJIS, etc) will have encryption turned on and will be password protected at all times. The encryption key will be maintained in a secure location by both the user and the ISO.

iPhone
iPhones are natively encrypted. These devices are required to be password protected and/or biometrically protected at all times.

E. Wi-Fi network encryption

All wireless access points owned by **Virtru** are required to be protected using Wi-Fi Protected Access 2 with Advanced Encryption Standard (WPA2-AES). This password will be changed quarterly and will not be shared with users that are not employees or authorized Business Associates. Any outside users are required to use guest access points.

Employees that access **Virtru** resources from home are required to use Wi-Fi Protected Access 2 with Advanced Encryption Standard (WPA2-AES) to protect their devices. This password should be changed quarterly.

F. Email encryption

Virtru requires the use of its secure, encrypted email service to communicate with our employees about their Personally Identifiable Information, and to communicate any sensitive data. All email communication that includes personally identifiable data, and potentially sensitive data will be encrypted.

Virtru uses only its secure, encrypted email service to communicate with clients about their Personally Identifiable Information.

Virtru forbids the use of chat, texting or instant messaging programs by devices that store PHI.

G. Enforcement

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
See *Sanction Policy*.

XXI. Assessments and Testing

A. Overview

The Security Rule of HIPAA mandates that covered entities implement appropriate information security policies and procedures to protect PI from "reasonably anticipated threats and hazards."

B. Penetration testing

Penetration testing of all servers containing PII will be conducted monthly by internal personnel, and by an external 3rd party at least annually or whenever there is a major system update. Testing shall validate the security of:

1. External connections
2. Operating systems
3. Applications
4. Databases
5. Network controls
6. Security procedures, including monitoring and incident response

C. Vulnerability assessment testing

Vulnerability assessments will be conducted periodically on all network-connected systems devices. Any vulnerability found must be corrected in a timely manner. Vulnerability assessments also shall be conducted when:

1. A new system, application or network is installed inside the Company
2. Changes are made to firewalls, VPNs or other security control tools
3. Changes are made to a web server's operating system
4. Changes are made to email servers
5. Configuration changes are made to databases
6. Configuration changes are made to critical applications
7. Changes are made to encryption scheme(s)

NOTE: *Vulnerability and penetration tests will not be conducted except with the prior approval of the ISO. No user will have vulnerability or penetration testing tools loaded onto any* ***Company*** *system without prior permission from the ISO.*

D. Wireless access testing

Testing of wireless access points (war-driving) shall occur regularly, to cover all wireless access points under the control of **Virtru**.

E. Password testing

Password cracking software shall be run periodically to validate the enforcement of password rules.

F. 3rd Party Security Management

A comprehensive list of 3rd parties with which the company does business with shall be maintained. Any 3rd party who handles or holds sensitive data or who provides a service which is critical to operations shall be required to assert that their own security practices and procedures meet or exceed that of the company's. Each 3rd party shall be assessed for conformance annually.

XXII. Use of Email, Internet, Messaging, Public Sites, Blogs, Social Media

A. Policy

Confidential, Private or Protected information and Internal Use information must not be transmitted across any unsecured outside network or path without proper controls. **Virtru** requires encryption for files and emails, or secured packaging for paper copies.

Users are responsible for ensuring that their use of these tools complies with all of **Virtru's** policies, and with applicable laws and regulations. This includes all employment policies such as sexual harassment, stalking, ethics and appropriate use.

These tools may not be used to access, send or receive, store or display:

1. Sexually explicit material
2. Confidential, Private or Protected Information or Internal Use material, except as meets the *Handling Rules* section
3. Viruses
4. Threats
5. Inappropriate or unlawful language, including:
    a. Offensive language
    b. Language inappropriate for the **Company** environment
6. Discriminatory or harassing language
7. Tools usable for hacking, password cracking, vulnerability scanning or penetration testing

These tools are the property of **Virtru** and are to be used only for **Virtru's** business. Access may be unavailable at any time, at the **Company's** discretion. Users must not assume that access to these tools will be available for incidental personal use.

All content transmitted over these tools is the property of **Virtru**. Content, including emails, may be inspected by **Virtru**. Such inspections will occur with the approval of the ISO or of the **Company** legal department. **Virtru** may monitor, filter or block content on these tools.

Users of blogs, social media sites such as Facebook, and other such tools must follow the guidelines outlined in **Virtru's** Social Media Policy. See *Social Media Policy*.

Users of blogs, social media sites such as Facebook, and other such tools must not represent their comments as coming from, or being representative of, the business or opinions of **Virtru**.

XXIII. Hardware

A. Definitions

Workstations: PCs, desktop computers, tablets and mobile computing devices that are located at **Virtru's** home office, or at remote locations. These devices are easily attacked and therefore must have access controls and anti-malware as specified in those sections of this document.

Servers: Devices that may or may not be housed at **Virtru** locations. Regardless of their location, these must secured in a manner that prevents them from being physically accessed without the appropriate level of security clearance.

B. Policy

A current copy of the *Organizational Chart/Electronic Asset Management Log* (**Risk Assessment**) will be kept at an off site location so it can be accessed quickly in the case of theft, fire, flood or other events that may make inventory information useful.

The ISO will keep a log of events noting when a physical security mechanism is repaired, replaced, installed, removed, modified, or maintained. This *Maintenance Log* will contain the: who, what, when, where, and why of the change and be kept in the **Security Documentation Library**.

Users of these devices are required to ensure that all appropriate protections are in place, including:

1. Physical security to prevent theft or misuse
2. Access controls suitable for the class of information on the device
3. Anti-malware
4. Keeping the devices locked to a desk or other secure location when outside

Virtru

5. Keeping control over backup media, as to minimize the possibility of theft or loss
6. Ensuring that the transport of these devices is secure and is safe from damage - for example, these devices should only travel in padded containers and should be locked and shut down during transit
7. Keeping all operating systems and tools up-to-date, with all updates and patches. Specific requirements for these topics are in the appropriate sections of this document

Virtru's devices must not be used by people who are not authorized, including family members and friends.

Software loaded onto such devices must follow the rules in the *Software* section of this document. In general, only approved software may be loaded, and shareware, games and other such software are not permitted.

International travel with these devices may require special approvals or configurations, especially in regards to encryption and licensed software. Before traveling internationally, users must contact the ISO to determine if such special considerations exist.

Connecting these devices to **Virtru's** networks must follow the rules in the *Networks* section of this document. In general, all such devices must be approved prior to connecting.

Remote access from these devices to **Virtru's** networks and devices must meet the controls specified in the *Networks* section of this document. In general, such access must be approved, and must have adequate controls over the security of information in transit.

Devices of these types that are owned by contractors, vendors or other third parties must meet all **Virtru** requirements prior to being connected.

C. Asset management

The ISO is responsible for maintaining an inventory of devices; as such he shall employ software to aid in the management of hardware and software asset. See *Handling Rules for the information classifications*

D. Enforcement

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

XXIV. Networks

A. Overview

Virtru's networks and devices shall designed, deployed and operated in a manner so as to provide proper levels of protection for the data being accessed and transported. Significant changes in network designs must be piloted before deployment.

Mechanisms must be in place to alert the ISO of possible attacks and breaches, to include:

1. Denial of service attacks
2. Improper access
3. Virus infections
4. Unauthorized software installations, email, FTP or other improper usage

Analysis must be conducted at least annually to validate the failure mode and recovery for all devices, network circuits and protocols. See *Change Logs* for details.

Responsibilities must be defined for:

1. Administration of network and communications connections
2. Operations of all devices
3. Monitoring
4. Timely review of audit logs and response to alerts or alarms
5. Review of unusual patterns of usage or activity

To minimize risks, any network connections or network segments should be disconnected when not in use.

B. Monitoring

Virtru uses AlienVault's Unified Security Management System to monitor all traffic on their network. Notifications are set to alert the IT staff of any unusual traffic and vulnerabilities, as well as log any security events that may occur.

C. Access control and physical security

Sites where **Virtru's** network equipment or communications lines exist are considered to be high-value and are subject to the access control and physical security rules

outlined in the *Physical Security* section of this document. In general, these rules will require:

1. Access limited to authorized personnel only
2. Physical security, including RFID or passcode controlled locks, are in place

D. Modifications, updates

Changes to the network architecture which affect the protections must be approved by the ISO. Examples of such changes include firewalls, wireless configurations, ports and proxies.

E. Documentation

The ISO shall maintain an accurate set of documentation of the networks and their components. This documentation is considered to be highly valuable and will be classified "Protected".

F. Network design

The goal for network design is to facilitate **Virtru's** business, while still providing protection for **Company** assets.

G. Segmentation

Virtru's networks will be segmented, in order to limit access to Confidential and Protected Information, without impacting the **Company's** business. There will be a guest network that will have no access to **Virtru's** Network Attached Storage, and other vital network resources.

H. Firewalls

Virtru's network and workstations in the DC office is protected using the Fortinet FortiGate 100D Firewall appliance. This device is configured to monitor and log all unusual traffic and warn **Virtru** of any network irregularities or attacks.

Definitions

Firewall: A part of the computer operating system or network that is designed to block unauthorized access while permitting outward communication. There are two different types of firewalls.

1. *Software Firewall:* Part of the operating system or can be a software add-on.
2. *Hardware Firewall:* Built into a router or a stand alone device. All computing devices will access a network through this point.

Firewall Settings

1. *Whitelisting:* Blocks all incoming traffic, and only allows traffic from good, or known IP addresses. The user will be required to authorize connections to their device.

2. *Blacklisting:* Authorizes all traffic as a default, and the user is responsible for denying unauthorized connections to their computing device from unrecognized or unknown IP addresses.

Software Firewall Policy

Virtru requires every device to have their internal software firewall activated at all times, and set to only allow whitelisted traffic. This will require the user to authorize any connections to their device. Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I. Internet

Connections to the Internet must be:

1. Approved by the ISO
2. Periodically reviewed and tested for vulnerabilities
3. Protected by firewalls, intrusion detection systems and anti-malware tools

Some Internet tools, such as FTP, Internet Relay Chat, Telnet and Remote Procedure Call are restricted in use and must be approved for use by the ISO.

J. VPN-remote access

Virtual private networks (VPNs) will be used for traffic flowing over public networks to ensure the proper level of protection of **Virtru's** data.

K. Wireless

All wireless connections must have WPA2 with Advanced Encryption Standard (AES) turned on. This applies to all networks for **Virtru's** home office, and all telecommuting employees.

L. Telework Policy

If a staff member is allowed to telework/telecommute, they must comply with the **Virtru's** various employment policies, remote security measures and use the provided web portal via HTTPs, VPN and SSL. They must also make sure their home WI-FI is encrypted properly.

If they are accessing sites while on an unsecure router, they must make sure the sites they visit have a valid SSL certificate before proceeding.

M. Patching of systems and applications

Microsoft Windows OS Patches

Security Policies and Procedures

To manage the patching of Microsoft Windows operating systems (OS), Windows Software Update Service (WSUS) is used. The WSUS server automatically checks for patches once a day not during business hours. Then downloaded patches are manually released from the WSUS server to be downloaded and applied on the workstations. The ISO will evaluate all patches before they are applied; workstations will not automatically download OS patches from the WSUS server and updates will not be automatically installed. Installation of OS patches is done within a planned downtime.

Apple OS Patches
All Macintosh Operating System (OS) patching will be done through the App Store, and is the responsibility of the individual user to install. These should be applied within one (1) week of release from Apple.

Linux OS Patches
These patches should be applied and tested in an app staging environment before they are applied systemwide. The User is required to document where they received the patch, who downloaded it, what version of patching they are using, and when the patch was applied to the system. This documentation should be submitted to the ISO upon completion of the patching.

iPhone iOS Patching
All iPhone (OS) patching will be done through the App Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Apple.

Android Phone Patching
All Android patching will be done through the Google Play Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Google.

Windows Phone Patching
All Windows Phone patching will be done through the Windows Phone Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Windows.

Patching of applications is done on a weekly basis, unless a zero-day exploit is found in an application that is used within the domain. If such an exploit is found and a patch is released for said exploit, an emergency planned downtime will be called for at the conclusion of the business day to patch the application in question.

N. Network hardening

Upon adding new devices to the network, installation procedures and set-up must be followed. Hardening will be done on network devices as well as systems (e.g. laptops, workstations and servers) and handled by the ISO or AISO.

Hardening will be broken down into the following categories which include, but are not limited to:

1. Preparation and installation
2. Updates to: software, firmware and hardware
3. Setting of appropriate account and auditing rules
4. Setting of appropriate security rules
5. Turning on the internal firewall
6. Turning on full disk encryption (If device will have access to PHI)
7. Other internal operations such as:
    a. Installation of appropriate software for workstation, server or laptop

The ISO will notify all affected staff when making changes to the hardening policy and will update the Security Policies and Procedures at that time. Written approval for hardening procedures above and beyond what is currently mandated is not necessary.

XXV. Physical and Environmental Protections

A. Definitions

Secure sites: These are locations that require the highest level of protection. These sites include:

1. Computing centers
2. Network connection points
3. Media storage locations
4. Locations containing platforms which carry high-value or critical information or transactions

Physical Security: These may occur within **Virtru** where the overall building is operated to a lower level of security, but a certain area is more controlled due to documents, assets or processes which occur in that area.

B. Secure Sites Policy

Secure sites shall be established for all computing centers and other locations where there is a concentration of high-value or sensitive information, systems or networks.

Sites will be designed and operated according to best practices and in consideration of threats appropriate to the site such as hurricanes, tornados, power outages and intruders.

This standard is not to be construed as a complete list of requirements for a secure site. It should be used in conjunction with expert advice, architects, fire marshals, OSHA and other regulations.

Separate, isolated areas will be created within the secure site for:

1. Media libraries
2. Electrical supplies and controls
3. Environmental and mechanical controls

Access to these sub-areas will be on a need-only basis. Critical assets and operations must be conducted in a secured area or secured site, with protections implemented in accordance with the risks and value of the assets, information and operations.

C. Data Centers

All data centers used by the company must provide proof that they meet or exceed the security requirements and standards of the company.

XXVI. Physical Security Policy

A. Entry Policy

All **Virtru's** workforce members are allowed access to the physical site at any time of the day, and any day of the week. The site is secured with an electronic door lock that accepts RFID cards and a numeric passcode. RFID cards are issued by the ISO or AISO by request and after approval.

B. Loss of RFID key

If a workforce member loses their RFID key, they will notify the ISO or AISO as soon as possible so the key may be deactivated. Any workforce member found to have violated

this policy may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

C. Mobile devices

Mobile devices (laptops, netbook, tablets, iPhones, iPads, etc.) must have the appropriate encryption. Devices must have a power-on password or PIN, data encryption, auto-lock and role-based access per user. See *BYOD Policy* (**Forms for Employees**).

D. Video monitoring

Virtru's main office is monitored by a video camera. The data is stored in the Network Attached Storage which is physically secured in a locked cage in the IT closet. This data is stored for up to one (1) month.

E. Alarm system

Virtru's main office is monitored by an alarm system. It is attached to all doors and windows, and requires a 4-digit pin plus a modifier to deactivate. Once triggered, there is a 45-second delay before the local authorities, ISO and CEO are notified by the monitoring company. ADT is the company that is responsible for monitoring **Virtru's** main office.

The alarm pin code is changed quarterly, or at the time that an employee is fired or leaves the Company.

Virtru requires that this alarm be set by the last person to exit the office, and should be active anytime there is not an authorized employee on the premises.

F. Fire protection

Fire protection meet all regulations, including federal, state and local. Fire extinguishers shall be deployed in accordance with regulations of OSHA and fire inspectors. Periodic testing of alarms, fire extinguishers and fire evacuation procedures shall be conducted.

XXVII. Software

A. Overview

This section outlines the standards applying to operating systems, applications, databases and other software tools.

B. Acquisition of software

It is up to the developer to decide which software tools they will require for their workstation. All regulated software will only be download from trusted sources, such as the Apple App Store, Windows Store, or directly from reputable websites, etc.

Unregulated software is allowed, but must be fully documented and approved for use by the ISO. Documentation will include:

1. The source of the software
2. When it was downloaded
3. Who downloaded it for use and;
4. The date the ISO approved the use of the software

All software for Windows OS devices is required to be screened for malware prior to installation.

Any unauthorized software must be approved and validated, or removed.

Users of workstations, netbooks, wireless and other personal devices must not install unapproved software.

C. Open Source Software

The use of open source shareware or open source freeware may only occur if:

1. It is not used in a production environment OR
2. Prior to use it is fully tested, documented and **Virtru's** personnel are assigned to support it. Checks to be performed include:
    a. Verify usage license (no strong or weak copyleft licenses)
    b. Review open CVEs and available patches
    c. Perform internal security evaluation
    d. Flag for external security evaluation during next penetration test
3. The source of the software is documented
    a. URL
    b. Project lead
    c. Contributors
    d. Whether the project is actively maintained
4. The ISO approves of the use

D. Documentation

Documentation for sensitive applications and the operating systems which run those systems shall be stored securely. Backups of all documentation shall be maintained off

site. Access to the documentation for sensitive applications and the operating systems will be on a need-to-use basis.

E. Change Control and Maintenance

All proposed changes to production systems must be registered in the companies issue tracking system. Changes shall be categorized as standard, normal, or emergency. Standard changes are those that are performed frequently and considered low risk. Standard changes are reviewed quarterly and pre-approved for the following quarter. Normal changes are those which are not performed frequently and may pose some risk to the business. Each normal change must be reviewed by a minimum of two super-admins, the CTO and/or VP of engineering prior to being made. Reviewers are responsible for assessing the impact of the change in regards to the functionality, availability, durability, and security of the system. If a consensus among reviewers is reached, the proposed change is sized, sorted, and executed through the standard engineering workflow. Emergency changes are those that are required to rectify some form of degradation of the system. Emergency changes must be reviewed by a minimum of two super-admins. If a consensus is reached, emergency changes can bypass the standard engineering workflow and be made immediately. All changes to production systems must be captured in the company's issue tracking system without exception.

F. Operating Systems

Only approved operating systems will be loaded onto **Virtru**-owned assets. Before major upgrades to systems, authorization by the ISO and AISO will be required.

Default settings must be reviewed prior to installation to identify any security vulnerabilities. These settings will be communicated with all workforce members, or they will surrender their devices to the ISO or AISO for configuration.

G. Applications

All applications, whether developed or purchased, must comply with **Virtru's** policies and protection standards. The information owner is responsible for ensuring that these requirements are included during the development or acquisition of software.

The protection requirements for applications include:

1. Access control
2. Authorization
3. Information classification
4. Storage controls
5. Backup and restoration
6. Confidentiality and integrity requirements
7. Audit logs
8. Privacy, export control and other such requirements

All product associated applications must use HTTPS to communicate with all remote hosts, both Virtru hosted services and external third parties. HTTP and other non-encrypted communications are not allowed under any scenario.

Virtru applications shall treat user credentials with the utmost sensitivity and must follow security best practices for storing and transmitting user credentials. All credentials which are shared with a client device must be sent over HTTPS or another encrypted communication channel. All user credentials which are stored in a data store, must be stored in a benign state so that leakage of information from the data store does not compromise user accounts.
All application logs must be sent to a central logging cluster for aggregation and analysis.

H. Configuration Management

Where possible, Virtru applications and infrastructure follow an immutable paradigm. All changes to production infrastructure and application code is deployed on a brand new Amazon Machine Image (AMI). This allows all changes which are deployed to be tracked and audited. This also means that no configuration or application code will be modified on a production instance. All application servers have osquery installed and configured to monitor key files on the system for any change (File Integrity Monitoring). Any changes to configuration are logged and sent to AWS Cloudwatch Logs, where they trigger an alarm and cause an email to be sent to the Virtru DevOps team for further investigation.

Where possible, Virtru utilizes Terraform, Ansible, and other similar tools to define their infrastructure as code. This allows the production infrastructure to be versioned in a git repository and easily audited for change over time.

I. Asset management for software

The ISO is responsible for maintaining an inventory of software; as such it shall employ software to aid in the management of software assets.

J. Enforcement

Any workforce member found to have violated these policies may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

XXVIII. Removable Media Device Policy

A. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of Confidential or Protected Information maintained by **Virtru** when it is stored, transferred or accessed on a removable media device. This policy also aims to reduce the risk of acquiring malware infections on computers operated by Company. Any questions or comments about this policy should be directed to the ISO

B. Scope

This policy covers all removable media that contains **Virtru's** data or that is connected to **Virtru's** network.

C. Definitions

Removable media: devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players or any other storage medium; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks.

Encryption: a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Malware: software of malicious intent/impact such as viruses, worms, and spyware.

D. Policy

Workforce members may use removable media in their work computers if they take all reasonable and prudent measures to ensure the safety and confidentiality of all information that is downloaded to any removable media or portable device

E. Using Removable Media Devices

PHI should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When

Protected and Confidential information is stored on removable media, it must be encrypted in accordance with **Virtru's** Encryption Standards.

The workforce member shall take all reasonable and prudent measures to physically secure all removable media or to portable devices. Users shall not open or attempt to open the encasement of any removable media or portable devices nor otherwise circumvent any lock system that secures the device or its components. Users should take reasonable measures to secure device at all time and report any lost or stolen removable media or portable devices immediately.

Workforce members may not copy information or other sensitive data onto personal devices, unless approved by management in conjunction with the *Confidentiality Agreement for Employees*.

F. Exceptions

Exceptions to this policy may be requested on a case-by-case basis by petition to the ISO.

G. Refusal

Virtru reserves the right to refuse the ability to connect removable media devices to the Company network if such media is being used in such a way that puts **Virtru's** systems, data, users and customers at risk.

H. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with **Virtru**.

XXIX. Application Recovery Plan

A. Overview

Virtru backs up of all production data hourly and stores it remotely on two separate Amazon Web Server (AWS) Accounts. These backups are a combination of both differential and full backups. These backups are durable a the same rate as S3 data, each snapshot is 99.99999% durable.

B. Scope

These policies apply to all production servers and data that **Virtru** is responsible for maintaining on behalf of our clients.

C. Data durability and reliability

Virtru uses Amazon S3 to provide a highly durable storage infrastructure designed for mission-critical and primary data storage. Amazon S3 redundantly stores data in multiple facilities and on multiple devices within each facility. To increase durability, Amazon S3 synchronously stores **Virtru's** data across multiple facilities before confirming that the data has been successfully stored. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Amazon S3 performs regular, systematic data integrity checks and is automatically self-healing.

D. Encryption

Virtru uses Server-side encryption to protect data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption by encrypting each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard (AES-256) to encrypt **Virtru's** data.

E. Load balancing

Virtru uses Amazon Web Services' Elastic Load Balancing (ELB) to automatically distribute incoming application traffic, to automatically route traffic across multiple instances. and multiple Availability Zones. This is used to insure that only healthy servers are receiving traffic.

F. Restoration of data

Restoration of production data is done on an as-needed basis. The following employees are responsible for restoration of the application if it is needed:

1. Reuven Gonzales, Lead Developer, or
2. Conor Gilsenan, Developer Ops.

The needed backup data will not be restored "on top of" the current "bad" data. The restores will be redirected to a new location, and first verified. Upon verification, the "bad" data will be removed from the drive, and stored and relabeled as "old data." Then the backup data will replace the "old data" on the drive. Once the restored data has been verified once more, the "old data" will be destroyed.

G. Testing and revision of plan

Once every quarter, after doing a full backup, **Virtru** will recover the saved data. During hours when the business is closed, we will operate the application using this recovered data in a test mode. The tests will consist of a set of tasks that are designed to exercise the main system functions to confirm that the data is usable and as up-to-date as we expected given the backups that were used to do the recovery. This testing process

should take an hour. The restore process should take an hour or two, once the files are retrieved.

If the process does not work as documented in our policy, it will be updated to reflect the actual procedure we need to implement to achieve successful recovery and operation.

Whenever we make changes to software or hardware, we will create/update and test using our *Inventory of Devices/Software Assets* and store this checklist in the **Security Documentation Library**.

XXX. Network Attached Storage and Workstation Backup Plan

A. Overview

Virtru recognizes that the backup and maintenance of data in the Network Attached Storage (NAS) and individual workstations are critical to operations. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

B. Policy

Virtru will be using a Synology DS1515+ Network Attached Storage for backing up all workstations, firewall logs, and video surveillance footage. This data will also be backed up to a Amazon Web Services Glacier account.

C. Backup software

Virtru uses Cloud Station software to perform all backups. This will be installed on all workstations and must not be disabled by the user for more than one (1) business day. The software will maintain one month of file versions for restoring purposes

D. Remote backups

Virtru will provide a Virtual Private Network (VPN) for employees to login to for backing up their devices. Credentials for the VPM will be provided to remote employees, and they will be expected to configure their devices properly. If they are unsure, or have issue in setup, the IT department will be available for configuration assistance.

E. Local backups

Virtru encourages all users to do daily local backups of their data. These backups are to be encrypted using the encryption standards listed below. Any local backups must be surrendered at the time an employee no longer is employed by **Virtru**.

F. Encryption of backups

The backups of data will be encrypted on the NAS using AES 256 bit encryption. Any local backups that employees make must be encrypted at a minimum of 256 bit encryption.

G. Restoring data

In the event that a workstation fails, is stolen, or is damaged whether physically or by malware. It is the policy of **Virtru** that this device will be replaced within 24 hours. The IT department will be responsible for reprovisioning this device, and testing that the workstation is functioning properly before giving the device to the employee.

H. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with **Virtru**.

XXXI. Information Integrity Management Policy

A. Overview

The other policies in this document contribute to the integrity of the data in our systems. Notably, the Data Backup Plan, the Access Control Policy, and the Malware Management Policy contribute to data integrity. In addition to these, we add the following policy elements.

B. Policy

Virtru will configure our applications software to use the available edits on data that is entered into our systems. These edits will check for internal data consistency, reasonableness of data, and logical relations among data items.

XXXII. Security Incident Management Policy

A. Overview

Virtru recognizes that, despite having reasonable security safeguards, we may have security incidents.

B. Procedures

To manage these incidents, **Virtru** will do the following:

1. We will train each workforce member to recognize the common telltale signs of a security incident. When a member of the workforce detects one of these signs, he/she will be responsible for notifying the ISO.
2. The ISO will maintain a set of tests to detect events in the system logs that may indicate security incidents. These tests will be written into a script and run against the system log on a daily basis or whenever needed. The tests currently are:
    a) Account creation/deletion
    b) High volume of unsuccessful logon attempts
    c) Alerts from our malware monitoring systems
    d) High volume of file or database access/creation/deletion activity for the time of day, or for day of the week
    e) Account activity at unusual times of the day or night
    f) Absence of expected log records of activity when expected
    g) Unusual level of record access for a given account
    h) Daily logs will be tested by the firewall in real time,
    i) User data will be reviewed weekly
    j) Logs for the past month will be retained. When anomalies are discovered, the script will provide a report that is immediately brought to the attention of the ISO or designee as a potential security incident.
    k) Account lock out due to excessive password retry failure.

The ISO will determine, in consultation with others if needed, whether an event is a security incident.

If an event is a security incident, the ISO (or designee) will proceed to contain and repair damage from the incident by working with staff, vendors, and Business Associates as needed. The security incident will be tracked in JIRA and treated as an application defect. A log of relevant actions taken to contain and repair the damage will be stored in JIRA. The permanent home of this log will be in the **Security Documentation Library**. The ISO will determine if the event involves a workforce member action that is covered under the sanction policy and will follow that policy. The ISO will determine if the event represents a security incident for which a Business Associate is responsible. If so, the ISO will follow our *Incident and Breach Policy* in this area.

C. Policy

If an event is a security incident, the ISO (or designee) will proceed to contain and repair damage from the incident by working with staff, vendors, and Business Associate relations in order to further deter future incidents of the same type.

XXXIII. Security Plan Review Policy

A. Overview

We recognize that our underlying security risk will change and our ability to manage this risk will improve over time. To ensure that we adjust our policies and procedures to take these two factors into account, we will review our Security Policies and Procedures annually. The ISO will lead this review and involve others as needed. Documentation of the review will be contained in a document called *Annual Security Review* and restored in the **Security Documentation Library** {or **Notebook**}.

B. Procedures

At a minimum, the review process will consist of:

1. Evaluating changes in the last year that may affect our Security Policy. These will include changes in:
    a) Number, sizes or locations of our business sites
    b) Our workforce size and composition
    c) Hardware/software
    d) State or federal laws that apply to us
    e) Type of medical insurance that we provide
2. Reading each Policy to determine whether or not the changes may affect it and/or the practices driven by the Policy. We will make a list of changes that need to be made, then write a paragraph describing how.
3. Creating a list of changes in Policies and/or Procedures that our **Company** will carry out.
4. Developing and implementing any changes in our Policies and Procedures on a timely basis.

Security Policies and Procedures

Appendices

Security Policies and Procedures

A. Change Logs

The Change Logs are logs and reports that are reviewed, at a minimum, twice a year. It provides information on programs available and which employees have access to which programs. The actual logs are found in the **Change Control Logs for Security** section of the documents.

1. Annual Security Review
2. Application/Database Change
3. Employee Access
4. Incident - Disaster
5. Maintenance
6. Media Sanitization
7. Operating System Changes Audit
8. Organizational Chart/Electronic Asset Management
9. Network Change
10. Physical Entry Access
11. Responsibility Change

B. Information Security Committee

Information Security Officer:
Will Ackerly
willackerly@virtru.com
(202) 577-3683

Information Security Committee:
Jordan Duggan
Jordan@virtru.com
(919) 696-7936

Reuven Gonzales, Director of Operations
Cell: (949) 878-6154
reuven@virtru.com

Conor Gilsenan, Operations Developer
Cell: 973-986-6650
conor@virtru.com

Disaster Recovery Plan for Virtru

We define a disaster as any event that affects our information systems and, as a result, substantially interferes with the operations of our business. Examples are fire, flood, hardware failure of critical elements (servers), software failures, theft, chemical/radiation hazard, and sabotage. Our definition of recovering from a disaster is taking all the actions needed to restore the systems to their normal operational state. Our plan to recover from disasters is described below.

1. What we will do to prepare to perform a disaster recovery:

    A. We will train the workforce to recognize and report a disaster.

    B. We will organize the workforce responsibilities so that during a recovery we are not dependent on only one person for any critical step.

    C. We will report disasters to the ISO and AISO. The ISO will make the formal determination as to whether or not to classify the event as a disaster.

    D. We will store paper backup copies of key disaster related documents with the offsite backups. These documents will include a List of Support Contacts – vendor, reseller, and/or support group contact information for all of our software and hardware.

    E. We will keep an *Inventory of Device/Software Assets* for [Name of Business]–– a detailed checklist for each asset, such as the server, PCs, the router, network switch, databases, and software programs containing tasks that must be completed to recover that asset. The list will include key data about the device including a party responsible for the recovery whose role is to diagnose and, if needed, repair, replace, and/or rebuild a device.

    F. We will have current copies of system data and software available at the off site location, as our data backup plan specifies.

2. Once the ISO (or designee) has certified a disaster, we will:

    A. Use the ISO or designee to facilitate the recovery. The facilitator will direct the recovery process, coordination and communication of the actions of the various parties that are involved in the recovery.
    B. Determine which devices/software (e.g. servers, PCs, power units, AC units) are not functioning normally, conferring with the appropriate staff, vendors, and other support personnel to make this determination. When in doubt about the status of the device, we will either use a test that is described in the IT Assets Recovery Checklist for the device/system or depend on the recovery responsible party to make this determination.
    C. Review the *Inventory of Device/Software Assets* for the devices to be recovered. Each checklist will have as an initial task, "Contact the appropriate parties responsible for restoring the devices/software to be recovered." Guidance and other recovery activities from these parties are key contributors to the recovery process.
    D. After all of the non-functioning assets have been restored, follow the instructions in the part of the Emergency Operations Plan that deals with what to do when the system is available again.

Organization

Emergency Planning & Crisis Management Team (**EPCMT**):

- Will Ackerly, CTO & ISO
- Jordan Duggan, VP of Product & Development & AISO
- Reuven Gonzales, Director of Operations
- Conor Gilsenan, Operations Developer
- Zack Nelson, Director of Development

Primary Disaster coordination handled through:

Crisis Manager 1:
Reuven Gonzales, Director of Operations
Cell: (949) 878-6154
reuven@virtru.com

Crisis Manager 2:
Conor Gilsenan, Operations Developer
Cell: 973-986-6650
conor@virtru.com

Other Members' Contact Information

- Zack Nelson 443-834-3791
- Payam Abedi 703-656-6227
- Tyler Biscoe 301-642-8844
- Jon Gilpen 303-358-6689
- Jason Ghent 803-658-6645

Off-Site Meeting Location

Used if team needs to meet to formulate an action plan.

If primary location is not accessible, we may need to operate from an off-site locations such as:

Employees' Home Offices
Jack Rose Restaurant

Extended off-site locations will be determined after assessing the severity of the disaster.

Disaster Recovery Timeframes

Maximum Tolerable Downtime (MTD)

The total amount of time our company is willing to accept for an outage or disruption, including all impact considerations. This guides our Crisis Management Team in determining the selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.

Recovery Point Objective (RPO)

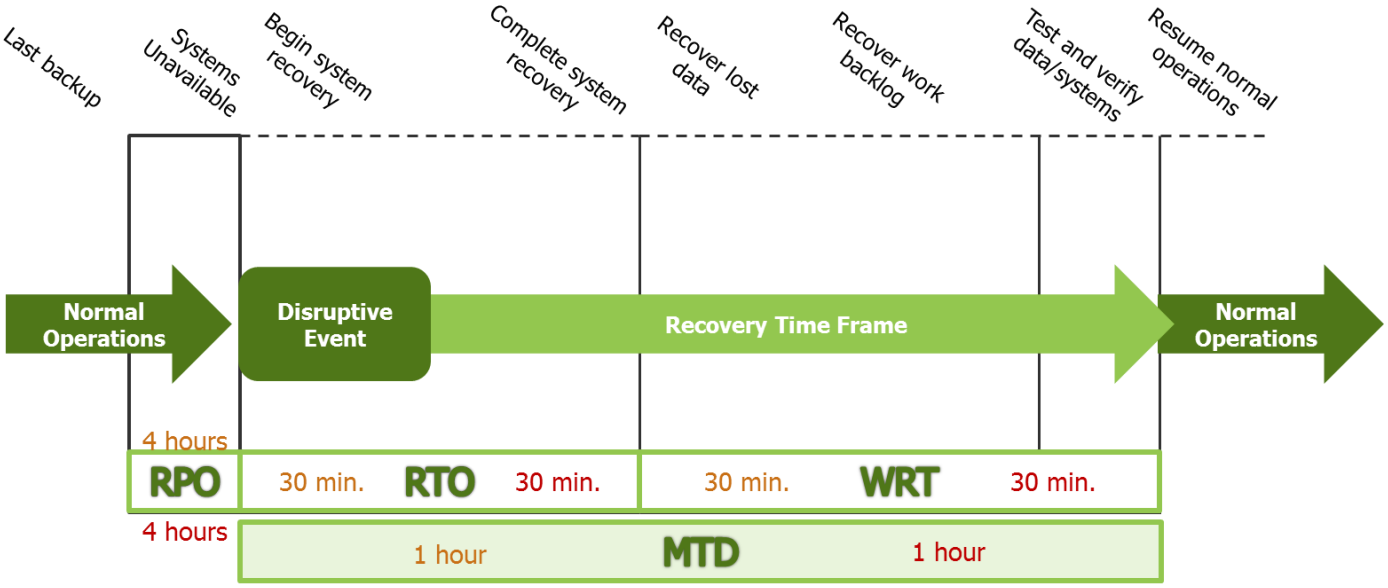
This is the point in time, prior to a disaster or disruptive event, which our company has accepted for data loss. RPO determines the frequency of our data backups. When determining RPO, we need to consider how much newly entered data we can afford to lose. *Therefore, if RPO is set to 4 hours, then we must have offsite backups maintained every 4 hours.*

Recovery Time Objective (RTO)

RTO determines the target time for recommencement of business activity. The Crisis Management Team will determine what business functions (i.e. telecommunications, web servers, etc.) should be restored based on priority.

Working Recovery Time (WRT)

This is the time our company will spend recovering lost data and work backlog, and testing and verifying data and systems. WRT usually is the difference between MTD and RTO.



Physical Security Example Times
Minor Disaster and Major Disaster

(See next page)

Disaster Timeframe Expectations

Internal Network
The server and network must be functioning in order for any of our other information systems to function. We could afford to be without the server/network for ten (10) minutes without materially affecting our business. If the server/network is down for longer than ten (10) minutes, staff will switch over the mobile tethering, or will go to an approved location to continue their work.

Production Servers
Production servers must be functioning at all times in order for our applications to work. We cannot afford to be without the production servers without materially affecting our business. Traffic will be automatically routed to another server via Amazon Web Services' Elastic Load Balancing.

Workstations
If a workstation crashes, we can easily use another one with only modest inconvenience. Ideally, we would like to replace/restore a workstation within 72 hours.

Printer and Fax
We have two multifunction printers. We can lose all printers for up to a week with little effect on data flow.

Email and Web Browser
Currently, we can function for no more than 10 minutes without email or web browsing. We will tether devices via smartphones after that time.

Wireless Network
We have a wireless network and the office depends on it for routine transactions. A backup router is available; it is preconfigured and encrypted using WPA2-AES.

IT Resources
We depend on the availability of certain employees and our IT service provider to diagnose and fix problems quickly. A chain of contacts is available in this document.

Power and HVAC Equipment
We depend on external power and environmental equipment (especially our AC unit) to maintain the power and environmental support for our system. Failure of either of these systems could inhibit the use of our IT systems, and could also stop us from doing business. These failures are not IT-specific risks. We are comfortable enough with the track record of these services not to need more than a short term UPS to allow us to smoothly shut the network down in the event of a sustained power outage. We have to yearly revisit the question of whether or not we need

more power/environmental backup to ensure that the satellite site will able to operate even if power/cooling at the main site is out.

Disaster Timeframes Table

{This is a sample. Please fill in according to Virtru's standards. Functions can include departments, as listed below, or they can include more specific tasks, such as invoicing.}

	Minor Disaster				Major Disaster			
Function	**MTD**	**RTO**	**WRT**	**RPO**	**MTD**	**RTO**	**WRT**	**RPO**
Physical Security (office/suite)	1 hour	30 minutes	30 minutes	4 hours	1 hour	30 minutes	30 minutes	4 hours
IT (server, hardware, equipment)								
Sales and Marketing								
Administration								
HR								

EVACUATION PLAN - during business hours:

For a disaster where you will need to **leave the building:**

If a disaster happens during normal business hours all Company employees will meet at **Jack Rose Restaurant, 2007 18th St NW, Washington, DC 20009.**

This will prevent Company employees from being in the way of emergency crews. A head count by managers will determine if all staff members have fully exited the building.

Headcount numbers will be brought to the ISO or CEO.

If the disaster happens after the meeting location has closed, employees will wait outside of the same address.

For a disaster where you will need to **stay in the building:**

If a disaster happens during normal business hours, all Company employees will meet in the **Basement**. A head count will determine if all staff members have fully exited the suite. See above for head count procedures.

{Please fill in the appropriate personnel for the following responsibilities}

Office/Evacuation Managers	Assembly Managers
Will Ackerly	John Ackerly
John Ackerly as Backup	Will Ackerly as Backup
System Shutdown Manager	**Back-up System Shutdown Manager**
Jordan Duggan	Jordan Duggan
Will Ackerly as Backup	Will Ackerly as Backup

Critical Operation Priority List

If or when a disaster happens, certain contacts will need to be made.

Operation	Employee in Charge	Action Plan
Current enrollment processes (any pending business)	Will Ackerly	Notify carriers of current situation—give cell number if needed.
Communications	Will Ackerly	eBlast to client list
IT—phones, faxes, e-mail	John Ackerly	Set up remote office
Payroll-Banking issues-Commissions	John Ackerly	Notify payroll/banking institutions of disaster and action plan

Potential Purchase List

If or when a disaster happens, certain items may need to be replaced:

1. 3 UPS (Uninterruptible Power Supply)(s)(Batteries)
2. Network Attached Storage (NAS)
3. Network Switch(s)
4. Network cable(s)
5. Power cable(s)
6. Power strip(s)
7. Monitor(s) / Monitor Cable(s)
8. Keyboard(s) / Mouse(s)
9. Firewall
10. Workstation(s) / Laptop(s)
11. Phone(s) & Headsets
12. Security Camera
13. Electronic Door Lock
14. Video Conference Microphones
15. Minifridge
16. Projector
17. Software
    a. OSX
    b. Windows
    c. Acrobat
    d. Office Suite
18. Paper
    a. Printer paper
    b. Sticky notes
    c. New Checks
19. Multifunction Color Printer
20. Office Furniture/Equipment
21. Carrier (Marketing) Supplies
22. Office Supplies

Fire Plan

EVACUATION PLAN - FIRE!

If the fire alarm goes off during business hours, **evacuate the building immediately**. If you discover a fire or smell heavy smoke inside building:
DO NOT ATTEMPT TO FIGHT THE FIRE!!

1. Pull fire alarm, evacuate the building and call 911 on the way out of the building

2. Perform head count at the designated assembly point

    - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.

3. Action Plan - developed by ***EPCMT***

    - Re-open based on damage
    - If the office must remain closed:
        - Notify employees and/or employees emergency contacts.
        - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Earthquake Plan

EVACUATION PLAN - Earthquake!

During an Earthquake

- **DO NOT USE THE ELEVATOR DURING AN EMERGENCY EVACUATION**.
- If you're indoors, stay there. Get under -- and hold onto --a desk or table, or stand against an interior wall. Stay clear of exterior walls, glass, heavy furniture, fireplaces and appliances. The kitchen is a particularly dangerous spot. If you're in an office building, stay away from windows and outside walls and do not use the elevator.
- If you're outside, get into the open. Stay clear of buildings, power lines or anything else that could fall on you.

After an Earthquake

- Perform head count at the designated assembly point
    - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
- Shut down systems, if time permits, see **Emergency Shutdown Procedures**
    - Check for fire or fire hazards. If you smell gas, shut off the main gas valve. If there's evidence of damage to electrical wiring, shut off the power at the control box.
    - If the phone is working, only use it in case of emergency. Likewise, avoid driving if possible to keep the streets clear for emergency vehicles.

- Be aware that items may fall out of cupboards or closets when the door is opened, and also that chimneys can be weakened and fall with a touch. Check for cracks and damage to the roof and foundation of your home.
- Listen to the radio for important information and instructions. Remember that aftershocks, sometimes large enough to cause damage in their own right, generally follow large quakes.
- If you leave home, leave a message telling friends and family your location.

- Action Plan - developed by ***EPCMT***
  - Re-open based on damage
  - If the office must remain closed:
    - Notify employees and/or employees emergency contacts.
    - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Tornado Plan

EVACUATION PLAN - Tornado!

If the city or county signal a tornado warning, move away from the perimeter of the building and any exterior glass.

DO NOT USE ANY ELEVATORS DURING AN EMERGENCY EVACUATION.

1. Move to the basement of the office suite.
2. Shutdown systems, if time permits, see **Emergency Shutdown Procedures**
3. Perform head count at the designated assembly point
    - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
4. Action Plan - developed by ***EPCMT***
    - Re-open based on damage
    - If the office must remain closed:
        - Notify employees and/or employees emergency contacts.
        - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Flood Plan

EVACUATION PLAN - Flood!

1. Evaluate the situation
    - Shutdown systems routine, see **Emergency Shutdown Procedures**
    - Perform head count
        - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
2. Action Plan - developed by ***EPCMT***
    - Remain open - *based on damage or location*
        - Relocate staff within suite
        - Evaluate IT requirements
    - Close - send staff home
        - Re-open based on damage
        - If the office must remain closed:
            - Notify employees and/or employees emergency contacts.
            - If there is any impact to customer operations, email all clients with a status update and recovery plan.

After Hours Plan

EVACUATION PLAN - after business hours

If the building is in a disastrous state after working hours, the **EPCMT** will notify employees. *See **Virtru** Phone Tree*.

If **re-opening** on a workday at the primary location:

1. Verify location is safe for operations - including systems
2. Communications
    a. Emergency Contact List
    b. Client Blast

If **NOT re-opening** on the following workday at the primary location:

1. The **EPCMT** must decide estimated length of time we will not be able to function
    a. If less than or equal to one day, office is closed.
        i. **[Name of Business]** will open the following work day
        ii. Verify location is safe for operations
        iii. Communications
            1. Emergency Contact List
            2. Client Blast

2. If office needs to move to secondary location or close for a **short** period of time.
    a. The **EPCMT** meets to develop a plan of action
    b. Determine the validity of systems
        i. If valid, move critical systems to secondary location
        ii. If not valid, retrieve necessary items and contact suppliers for new systems
            1. Restore systems from backups
            2. Restore connectivity
                a. Skeleton crew of selected staff members (possibly several from each department)

c. Communications

i. Emergency Contact List

ii. Client Blast

3. If office needs to move to secondary location or close for a **longer** period of time:

a. The **EPCMT** meets to develop a plan of action

b. Determine the validity of Systems

i. If valid, move critical systems to secondary location

ii. If not valid, retrieve necessary items and contact suppliers for new systems

1. Restore systems from backups
2. Restore connectivity

ii. Determine staff needs - full or partial capacity

iii. Communications

1. Emergency Contact List
2. Client Blast

Emergency Contact List

Emergency services—call 911	
Police	000-000-0000
Fire	000-000-0000
Poison Center	800-222-1222
Building	
Building Owner	000-000-0000
Alarm Company	000-000-0000
Cleaning Company	000-000-0000

Technical Issues	
Technologies Company	000-000-0000
Website-Programmer	000-000-0000
Miscellaneous Internal Operations/Vendors	
Staffing Companies	000-000-0000
UPS	000-000-0000
Bank	000-000-0000
401K Company	000-000-0000
Payroll Company	000-000-0000

Emergency Shutdown Procedures

If an electrocution occurs while working in server room, staff will pull all of the UPS cords from the outlet by the interior door. If that outlet is inaccessible due to fire or victim's position, staff will shut off the power at the breaker, located in the basement on the wall to the left of the TV.

If there is a fire within the building or suite, staff should concentrate on notifying authorities.

If there is severe flooding that threatens to affect the server room, staff will shutdown and unplug all equipment and move it to the second story platform of the suite.

BRIGHTLINE

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013

The Certification Body of BrightLine hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

ServiceNow, Inc.

for the following scope of registration

The scope of the ISO/IEC 27001:2013 certification is limited to the information security management system (ISMS), which supports ServiceNow as a provider of cloud-based solutions that define, structure, manage and automate services across the global enterprise, as well as all supporting resources including global data center operations and infrastructure, applications, end-user services, and product development, and in accordance with the Statement of Applicability, approved July 28, 2015. Assets within scope of the ISMS include: internal information assets, customer data, software, hardware, people, and physical assets to host, support and operate the cloud-based solutions. The data centers in the following locations house the infrastructure used to deliver the cloud-based solutions: Virginia, California, Florida, Washington, Montreal, Toronto, London, Amsterdam, Geneva, Zurich, Sydney, Brisbane, Singapore, Hong Kong, São Paulo and Campinas. Additionally, ServiceNow uses Amazon Web Services (AWS) to host some ServiceWatch customers. Excluded from the scope are all operations of third party data centers and AWS.

the scope of this certification includes the following locations:

Santa Clara (HQ): 3260 Jay Street, Santa Clara, California, 95054, United States
San Diego: 4810 Eastgate Mall, San Diego, California, 92121, United States
Kirkland: 4400 Carillon Point, Kirkland, Washington, 98033, United States
Orlando: 3501 Quadrangle Blvd, Suite 150, Orlando, FL 32817, United States
Amsterdam (EMEA HQ): Hoekenrode 3, 1102 BR Amsterdam, The Netherlands
London: 3rd Floor, Future House, The Glanty, Egham, Surrey, TW20 9AH, United Kingdom
Sydney: Level 21, 50 Bridge St, Sydney, New South Wales, 2000, Australia

Certificate Number: **1980700-4**

ISO 27001 CERTIFIED BY BRIGHTLINE

ANAB ACCREDITED

Authorized by:

Christopher L. Schellman
President, BrightLine
1300 N. West Shore Blvd, Suite 240
Tampa, Florida 33607, United States
www.BrightLine.com

Issue Date	Original Registration Date	Expiration Date	Certificate Version
September 29, 2015	December 17, 2012	September 28, 2018	Version 4

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by BrightLine.
3. ISO 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. BrightLine expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of BrightLine and is bound by the conditions of contract. The authenticity of this certificate can be validated at www.BrightLine.com/Certificate-Directory.

vCLOUD GOVERNMENT SERVICE

Compliant cloud solutions built for government agencies

Whether spurred by the need to increase efficiency, meet government mandates or deal with rapidly expanding data sets and workloads, more and more agencies are moving some or all of their applications or infrastructure to the cloud. However, for many agencies, the most cost-effective, secure and efficient solution is a hybrid cloud model that allows them to not only leverage their existing investments in IT infrastructure, but also extend their systems seamlessly to the technology platform that best meets their needs.

VMware®, the global leader in virtualization and cloud infrastructure, and QTS, a trusted cloud operator and leading provider of hybrid cloud services and managed hosting for government agencies and enterprises, have partnered to deliver VMware vCloud® Government Service provided by Carpathia™ (A QTS Company).

vCloud Government Service is an enterprise-class hybrid cloud service designed to run new and existing applications in exactly the same way, giving government organizations application and data mobility. Being able to use existing people, processes, tools, and automation enables government organizations to focus on the benefits of the cloud to their mission, rather than taking time and resources to re-architect for new infrastructure. Federal organizations can securely extend their data centers to the cloud quickly and confidently, using an integrated cloud infrastructure with the security of a JAB-based FedRAMP Provisional Authorization.

KEY FEATURES

Robust Security and Compliance

- vCloud Government Service is a secure cloud platform that enables customers to maintain security and data protection that meets a broad range of regulations, standards, and best practices including FedRAMP, International Traffic Arms Regulations (ITAR), FIPS 140-2, and AT 101 SOC Type 2.

Efficiency and Manageability

- Agencies can write, deploy, and manage applications in the cloud in the same way they do today, without making any changes or additional investments. With management tools consistent across on premises and cloud environments, you can accelerate application deployments, streamline the deployment and update process, leverage pre-built components, and reuse application models across environments, and clouds.

Seamless Network Integration

- vCloud Government Service is built on a seamless virtualized network that is quickly customizable to support your application and security needs. Network virtualization allows you to configure your firewalls and network as if they were in your own data center so that you can replicate the network your applications need to operate. Get common identity and access management across your onsite and offsite cloud locations.

BENEFITS

- Ease of Use – Leverage your existing investments in applications and infrastructure and avoid the complexity of re-architecting for public cloud infrastructure
- Secure and Compliant – Secure cloud platform, with security controls designed to meet the unique requirements of government customers, most notably the FedRAMP standards
- Hybrid – True hybrid cloud solution enables both onsite and offsite IT environments to run new and existing applications seamlessly
- Fastest Path to Cloud Value – Use a common platform to leverage internal and external cloud resources without having to retrain your staff, and lower overall costs

Why vCloud Government Service?

vCloud Government Service has a FedRAMP Provisional Authority to Operate (P-ATO) and is generally available to U.S. government and defense organizations. It can be used for a variety of applications and workloads including:

- Test and development
- Packaged application hosting
- Backup and Disaster Recovery
- Web hosting and customer service
- On-demand data center expansion

Trusted Cloud Services

QTS is redefining the industry with trusted cloud services that leverage innovation to improve the flexibility, scalability, and cost-effectiveness of cloud services.

- We are a trusted cloud operator with past performance serving the government market -- including DoD, Civilian and Intelligence agencies -- across multiple programs and applications
- QTS data centers deliver the highest levels of security and compliance, and meet many compliance standards including FISMA, DIACAP, PCI, and HIPAA
- We hold a number of certifications and accreditations across multiple federal agencies and programs and support over 50 Federal systems holding active Authorizations to Operate (ATO)

Security

vCloud Government Service operates with a FedRAMP Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB). Built with a defense in-depth strategy that puts our customers' critical applications and data in the innermost ring, our people, processes and procedures ensure 100 percent compliance at implementation and through the lifecycle of the project.

Hybrid Options

vCloud Government Service is a true enterprise-class hybrid cloud service, offering a seamless platform for migrating and managing workloads between dedicated virtualized environments, on-premise infrastructures, third-party data centers and the cloud.

ABOUT QTS

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center solutions and fully managed services, and the owner of Carpathia Hosting, a leading provider of hybrid cloud services and managed hosting. QTS' integrated technology service platform of custom data center (C1), colocation (C2) and cloud and managed services (C3) provides flexible, scalable, secure IT solutions for web and IT applications. QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for data center owners and operators. QTS owns, operates or manages 25 data centers and bsupports more than 1,000 customers in North America, Europe and Asia Pacific.

March 10, 2016

State of Utah Division of Purchasing
3150 State Office Building
Capitol Hill
Salt Lake City, Utah 84114

Mr. Hughes:

As a privately owned company, Carahsoft Technology Corp. does not report to D&B. As such, the information in D&B is incorrect. To support you to determine that we have the financial resource to perform the contract we provide you the following information.

We are a stable, conservative and profitable company. Carahsoft continues to grow as noted by our year over year revenue below:

2010 $820 Million
2011 $1.12 Billion
2012 $1.46 Billion
2013 $1.81 Billion
2014 $2.45 Billion
2015 $3 Billion

We currently employ close to 500 employees.

To support you to determine that we have the financial resource to perform the contract we provide you the following information:

We maintain a $25M line of credit available (currently 100% available) with Xenith Bank. I have included a recent banking clarification letter from Xenith.

Mr. Joe Humphries is the Regional President and can be reached at 703-869-3610 if you need any information from him.

We have received numerous accolades including:

- For the 6th consecutive year CRN's 2012 Fast Growth List
- Washington Business Journal's 2012 List of Largest Government Contractors in Metro DC
- Third consecutive year Washington SmartCEO magazine's 2012 Future 50 list which recognizes the metro areas fastest growing companies.

Should you require additional details please call me and I can discuss our confidential financial information with you or provide you trade references that can further assist you.

Sincerely,

Jillian Dewey Szczepanek
Controller

dun & bradstreet

Carahsoft Technology Corp. DUNS: 08-836-5767

Credit Information

Risk Summary

Risk of Late Payment

Risk of late payment is based on the following prioritized factors in addition to other information in D&B's files:

- Proportion of slow payments in recent months
- Higher risk industry based on delinquency rates for this industry
- Increase in proportion of delinquent payments in recent payment experiences
- Proportion of past due balances to total amount owing
- Evidence of open liens

Indications of slowness can be the result of disputes over merchandise, skipped invoices, etc.

Payment Performance Trend

The payment performance trend for this company is Increased . Payment Trend currently is Increased compared to payments three months ago. The most recent payment information in D&B's files is:

- Payments currently: 11 days beyond terms
- Payments 3 months ago: 19 DAYS BEYOND terms
- Industry average: 5 DAYS BEYOND terms

*Note: Payments to suppliers are averaged weighted by dollar amounts.

Credit Limit Recommendation

Recommendation Date: 11/18/2015

Risk Category
High

Conservative Credit Limit
$0

Aggressive Credit Limit
$0

Company Profile

Chief Executive:
DIRECTOR(S): THE OFFICER(S)

Type of Business: NA

Years in Business: NA

Annual Sales:

Line of Business:
Whol computers/peripherals

1000000000

Employees Total: 500

Legal Filings and Other Important Information

Bankruptcies:	None	**Negative Payment Experience:**	None
Judgements:	0	**Negative Payment Experience Amount:**	None
Liens:	3		
Suits:	None	**Payments Placed for Collection:**	0
Suits/Judgments/Liens Amounts:	None		

The public record items reported may have been paid, terminated, vacated or released prior to the date this data is transmitted. Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

Special Events

We currently do have any information to be displayed for this business.

This report is prepared and provided under contract for the exclusive use of

This report may not be reproduced in whole or in part by any means of reproduction.

Payment Trends

Summary

Address:
1860 Michael Faraday Dr, Suite 100
Reston, VA 20190

Primary Industry SIC:
5045

D-U-N-S Number:
08-836-5767

Description:
Whol computers/peripherals

This is a **single** location.

Payment Activity

Total payment Experiences in D&Bs File:	48
Payments Within Terms: (not dollar weighted)	72%
Total Placed For Collection:	NA
Average Highest Credit:	$2,379,615
Largest High Credit:	$20,000,000
Highest Now Owing:	$20,000,000
Highest Past Due:	$4,000,000

Indications of slowness can be the result of dispute over merchandise, skipped invoices, etc. Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

PAYDEX® ®

3 Month PAYDEX®

75

When weighted by dollar amount, payments to suppliers average 8 days beyond terms terms.

Based on payments collected over the last 3 months

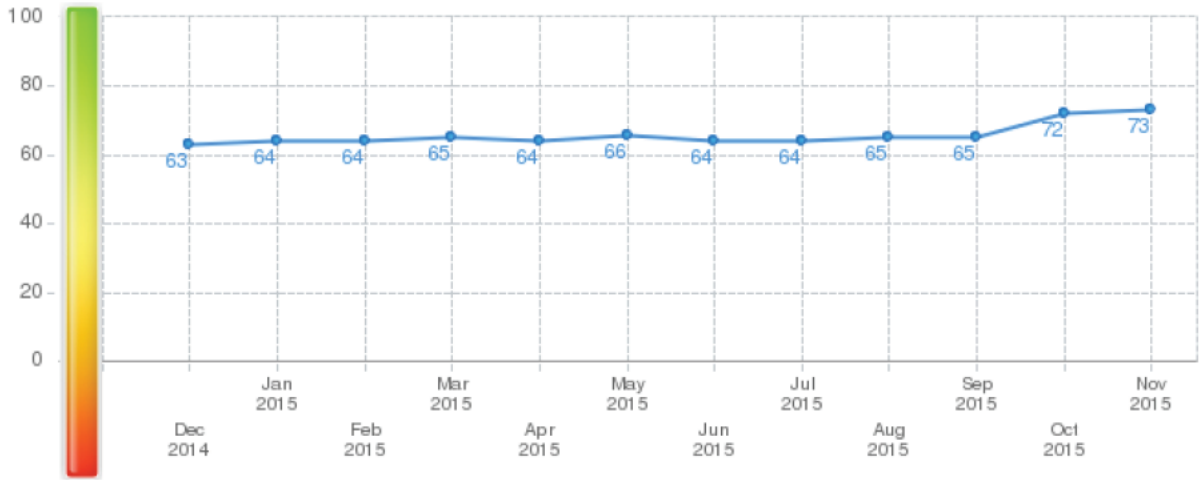
24 Month PAYDEX®

73

When weighted by dollar amount, payments to suppliers average 11 days beyond terms terms.

Based on payments collected over the last 24 months

PAYDEX ® Trends - This Company, 12 Months

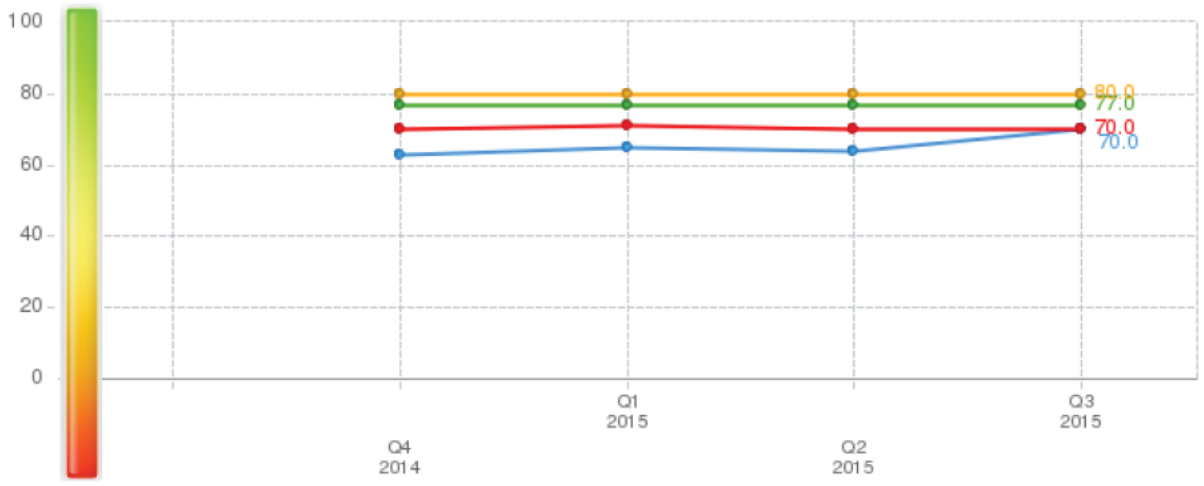


This Company (73)

Based on payments collected over the last 12 months.

- Current PAYDEX® for this Business is 73 , or equal to 11 days beyond terms terms
- The 12-month high is 73 , or equal to 11 DAYS BEYOND terms
- The 12-month low is 63 , or equal to 11 DAYS BEYOND terms

PAYDEX ® Score Comparison - This Company to Primary Industry Comparison, 4 Quarters



- My Company (73)
- Industry Upper Quartile (80)
- Industry Median (77)
- Industry Median (70)

Based on payments collected over the last 4 quarters.

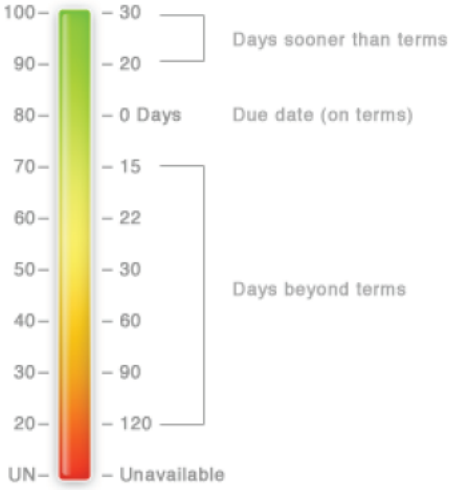
- Current PAYDEX® for this Business is 73 , or equal to 11 days beyond terms
- Current PAYDEX® for this Business is 77 , or equal to 5 DAYS BEYOND terms

- Industry upper quartile represents the performance of the payers in the 75th percentile
- Industry lower quartile represents the performance of the payers in the 25th percentile

Business Payment Habit by Amount of Credit Extended, 24 Months

$ Credit Extended	% of Payments Within Terms	# Payment Experiences	Total $ Dollar Amount
Over 100,000	73%	24	$90,200,000
50,000-100,000	100%	1	$85,000
15,000-49,999	27%	5	$110,000
5,000-14,999	73%	4	$27,500
1,000-4,999	100%	1	$2,500
under 1,000	100%	3	$400

How to Read the D&B PAYDEX ® Score



Risk Interpretation

	80 - 100	LOW risk of late payment (averages prompt to 30 days within terms)
	50 - 79	MEDIUM risk of late payment (averages 30 or less beyond terms)
	0 - 49	HIGH risk of late payment (averages 30 to 120 days beyond terms)

©Dun & Bradstreet, Inc. 2015. All rights reserved.

AODocs Terms of Service - Version published on the Web Site

TERMS OF SERVICE

These Terms of Service **("Terms")** are a legal agreement between Altirnao, Inc., herein **"Altirnao",** having an office and place of business at 221 Kearny Street, Suite 300, San Francisco, CA 94108, USA, and the person or entity agreeing to the terms herein **("Customer", "You" or "you").** By using or accessing any part of A0Docs (the **"Service"),** You agree that You have read, understand, and agree to be bound by all of the terms and conditions contained herein. If You do not agree to these Terms, You must not use or access the Service. If You are entering into this Terms on behalf of a company, You represent that You have the authority to bind that company to these Terms. If You have purchased a license to use A0Docs through an Altirnao reseller, You also agrees to comply with the terms of any agreement between You and such reseller. In the event of an inconsistency between these Terms and any such reseller agreements, these Terms shall control.

Description of Service

AODocs is an online document management solution for Google Apps. The Service is offered and provided subject to these Terms and solely for Your business purposes. You may connect to the Service using any Internet browser supported by the Service.

The Service requires one or more Google Apps for Business account that will be the owner(s) of all files stored and managed by the Service. The Service stores all the files that it stores and manages for You in the Google Drive account(s) that You will assign to AODocs when You deploy AODocs. You understand and acknowledge that You are solely responsible for obtaining the Internet access and all equipment necessary to use the Service, for appropriately configuring Your Google Apps account(s) and for allocating a sufficient number of accounts and sufficient Google Drive storage space to allow proper operation of the Service, as per the recommendation of Altirnao's technical support or product documentation. You also understand and agree that content you store through your use of the Service will be made available to Google as part of Google providing the Google Apps service. All fees associated with the foregoing shall be paid by You.

Modifications

To these Terms: Altirnao reserves the right to update and change the Terms of Service upon notice from time to time. You will be provided notice of any such modification by electronic mail or by the publishing of such on the website http://www.aodocs.com/terms-of-service. You may terminate your use of the Service if the Terms are modified in a manner that substantially affects your rights in connection with use of the Service. Your continued use of the Service after any such changes shall constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at http://www.aodocs.com/terms-of-service.

To the Service: Altirnao may make changes to the Service from time to time. Altirnao will notify you of any material changes or modifications. Any updates, upgrades, additions or new features to the Service, including the release of new tools and resources, shall be subject to these Terms and may require you to agree to additional terms and conditions.

Use of the Service

Access to Service: Access to the Service is only available to the Customer and the end users **("Users")** to whom Customer has purchased individual user licenses and granted access. Upon registration with Altirnao, Customer will specify the email address of a Google Apps account (the **"Account"),** which will be granted access to the Service. Customer is solely responsible for granting the Service access to Customer's Google Apps files and revoking such access when Customer ceases use of the Service. Customer is responsible for maintaining the confidentiality of Customer's password. Customer agrees not to share its password with anyone other than Users, let anyone else access its password or do anything else that might jeopardize the security of its password. Customer agrees to notify Altirnao if Customer's password is lost, stolen or disclosed to an unauthorized third party, if there is any unauthorized use of its password or Account, or if Customer learns of any other breach of security in relation to the Service. Customer is solely responsible for any and all activities that occur through the use of Customer's Account.

License to Customer: Subject to Customer's compliance with these Terms and the Google Acceptable Use Policy (available at https ://cloud.google .com/terms/aup), including, without limitation, Customer's payment of all applicable fees, Altirnao hereby grants Customer a limited, revocable, non-transferable non-exclusive, non-sublicensable license to access and use the Service, solely for Customer's own internal use, and not for timesharing, application service provider or service bureau use.

Customer is at all times fully responsible and liable for all acts and omissions by Users to whom Customer has granted access to the Service and Customer agrees to indemnify Altirnao for all claims and losses related to any such acts and/or omissions.

Each user license ordered by Customer is specific to the email address of only one User and, once granted to that User, may not be transferred or reassigned to any other user unless the User originally granted the license will no longer use the Service. Any such transfer or reassignment is permanent and Licensee shall not permit the original User to use the Service after such User's license has been used by a different User.

Altirnao reserves the right to terminate unpaid Accounts and Accounts that are inactive for a continuous period of ninety (90) days. In the event of any termination, all data associated with such Account will be deleted and Customer shall be responsible for revoking the Service's access to Customer's Google Apps domain data and files. Altirnao will provide Customer with prior notice of such termination and will send a data backup to Customer by email. In case of Accounts with more than one User, if at least one of the Users is active, the Account will not be considered inactive.

Restrictions on Use

Restrictions on Use of AODocs: In addition to all other terms and conditions contained herein, you shall not and shall not permit others to:

1. copy, modify, adapt, translate or otherwise create derivative works of the Service;
2. reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Service;
3. rent, lease, sell, assign or otherwise transfer rights in or to the Service;
4. remove any proprietary notices or labels from the Service;
5. use, post, transmit or introduce any device, software or routine which interferes or

attempts to interfere with the operation of the Service.

6. use the Service for spamming or any other illegal or unauthorized purpose or engage in illegal or deceptive trade practices; or

7. otherwise use of the Service in violation of any laws in your jurisdiction (including but not limited to copyright laws).

8. use the Service for High Risk Activities;

9. process or store any content on or through the Service that is subject to the International Traffic in Arms Regulations maintained by the Department of State.

10. if you are (or become) a Covered Entity or Business Associate, as defined in the Health Insurance Portability and Accountability Act **("HIPAA"),** use the Service for any purpose or in any manner involving Protected Health Information (as defined in HIPAA) unless you have received prior written consent to such use from both Google and Altirnao.

11. use the Service as a way to circumvent your obligation to provision one Google Apps End User Account for each User.

This list of prohibitions provides examples and is not complete or exclusive.

Restrictions on Use of Google Apps: You understand and agree that your use of the Service requires the use of Google Apps. You agree that you shall not and shall not permit others to:

copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract the source code of Google Apps or any component thereof;

use the Google Apps or any component thereof for uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of Google Apps or any component thereof could lead to death, personal injury, or environmental damage;

sublicense, resell, or distribute Google Apps or any component thereof;

use Google Apps or any component thereof to create, train, or improve (directly or indirectly) a substantially similar product or service, including any machine translation engine;

access Google Apps or any component thereof in a manner intended to avoid incurring fees;

use Google Apps or any component thereof to operate or enable any telecommunications service or in connection with any application that allows end users to place calls to or to receive calls from any public switched telephone network; or

process or store any data that is subject to the International Traffic in Arms Regulations maintained by the U.S Department of State or any other applicable law.

Altirnao reserves the right to suspend or terminate your access to Service with or without cause and with or without notice, for any reason or no reason, or for any action that Altirnao determines is inappropriate or disruptive to the Service or to any other user of this Service. Google may suspend your Google Apps account if: (a) your use of Google Apps is in violation of Google's Acceptable Use Policy, which could disrupt: (i) Google Apps; (ii) other users' use of Google Apps; or (iii) the Google network or servers used to provide Google Apps services; or
(b) there is unauthorized third party access to Google Apps.

You acknowledge and agree that Altirnao, in its sole discretion, with or without notice, may establish or revise from time to time general practices and limits concerning your use of the

Service, including without limitation, establishing the maximum number of Google Drive operations that can be done on your behalf in a given period of time. In addition, Altirnao may limit, without notice, the volume of e-mail forwarding or file downloading from the Service in response to unreasonable activity (such as spamming).

Altirnao may report to law enforcement authorities any actions that may be illegal, and any reports it receives of such conduct. When legally required or at Altirnao's discretion, Altirnao will cooperate with law enforcement agencies in any investigation of alleged illegal activity associated with the Service or on the Internet.

Unauthorized use of any trademarked, copyrighted or patented materials contained in the Service may violate certain laws and regulations.

You agree to indemnify and hold Altirnao and its officers, directors, employees, affiliates, agents, licensors, and business partners harmless from and against any and all costs, damages, liabilities, and expenses (including attorneys' fees and costs of defense) Altirnao or any other indemnified party suffers in relation to, arising from, or for the purpose of avoiding, any claim or demand from a third party that your use of this Service or the use of Service by any person using your Account (including without limitation, Your Content (as defined below)) violates any applicable law or regulation, or the copyrights, trademark rights or other rights of any third party.

Suspension

Altirnao reserves the right to suspend or terminate Customer's access to the Service with or without notice if Altirnao reasonably determines that:
(a) there is a threat or attack on the Service (including a denial of service attack) or other event that may create a risk to the Service, Altirnao, Customer, or any user of the Service;
(b) Customer's or its users' use of the Service or Customer Content disrupts or poses a security risk to the Service or any user of the Service, may harm Altirnao's systems, or may subject Altirnao or any third party to liability;
(c) Customer or any User is using the Service for fraudulent or illegal activities;
(d) Customer or any User is causing performance disruptions in the Service or in Google Drive by using the Service in a way that is not recommended in the performance guidelines published in the Service's documentation or by ignoring performance recommendations provided by Altirnao's technical support;
(e) subject to applicable law, Customer has ceased to continue Customer's business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding;
(f) Customer or any User is using the Service or other Altirnao property in breach of this Agreement;
or (g) Customer is in default of its payment obligations hereunder (collectively, "Service Suspensions"). Altirnao will make commercially reasonable efforts, circumstances permitting, to provide written notice of any Service Suspension to Customer, and to provide updates regarding resumption of Customer's access to the Service following any Service Suspension.

Subscription terms

Customer agrees to pay the subscription fee applicable to Customers and its Users use of the Service. Such fees will be paid on a periodic basis as agreed to Altirnao or to your Altirnao reseller as agreed when you registered for the Service.

In case of non-payment for any reason (including, if applicable, Altirnao's inability to charge your credit card or other payment method for any reason) or any violation of these Terms, Altirnao shall be entitled – without liability – to immediately suspend Customer's and Users' access to the Service. If you purchase your license to use the Service from Altirnao, you hereby expressly agree that Altirnao is permitted to bill you for the applicable fees, any applicable tax and any other charges you may incur in connection with your use of the Service, or charge such fees to your credit card or other payment method designated on your initial registration with the Altirnao at regular intervals for the remainder of the term of these Terms. If you cancel your Account at any time, you will not receive any refund.

Customer agrees that Customer's paid use of the Service is neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public or private comments made by Altirnao or any Altirnao reseller regarding future functionality or features.

Intellectual Property

Customer hereby acknowledges and agrees that, subject to the limited rights granted hereunder, Altirnao (or its licensors) own all legal right, title and interest in and to the Service, including, without limitation, any Intellectual Property Rights or other proprietary rights which exist in the Service (whether such rights are registered or unregistered, and wherever in the world those rights may exist) **("Our Technology").** For purposes of these Terms, "Intellectual Property Rights" means, on a worldwide basis, any and all now known or hereafter known (a) rights associated with works of authorship including copyrights and moral rights, (b) trademark and trade name rights and similar rights, (c) trade secret rights, (d) patent rights and other industrial property rights, (e) intellectual and industrial property rights of every other kind and nature and however designated, whether arising by operation of law or otherwise, and (f) all registrations, applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter existing, made, or in force (including any rights in any of the foregoing).

Our Technology may not be copied, modified, reproduced, republished, posted, transmitted, sold, offered for sale, or redistributed in any way without our prior written permission and the prior written permission of our applicable licensors. You must abide by all copyright notices, information, or restrictions contained in or attached to any of Our Technology. Nothing in these Terms of Use grants you any right to receive delivery of a copy of Our Technology or to obtain access to Our Technology except as generally and ordinarily permitted through the Service according to these Terms. Furthermore, nothing in these Terms of Use will be deemed to grant, by implication, estoppel or otherwise, a license to Our Technology. Certain of the names, logos, and other materials displayed on the Service constitute trademarks, trade names, service marks or logos **("Marks")** of Altirnao or other entities. You are not authorized to use any such Marks. Ownership of all such Marks and the goodwill associated therewith remains with and will inure to us or those other entities. To the extent indicated, any use of third party software provided in connection with the Service will be governed by such third parties' licenses and not by these Terms of Service. Furthermore, any comments, ideas and/or reports about the Service that you provide to us, whether in written or electronic form **("Feedback"),** shall be considered our proprietary and confidential information, and you hereby irrevocably transfer and assign to us all intellectual property rights embodied in or arising in connection with such Feedback, and any other rights or claims that you may have with respect to any such Feedback.

Ownership & Privacy

As between You and Altirnao, you retain all right, title and interest in any and all data, files, attachments, text, images, personally identifiable information, and other content that You and Your Users upload or submit to the Service (collectively, **"Your Content").** You may not upload, post or otherwise make available through the Service any material protected by copyright,

trademark, or any other proprietary right -without the express permission of the owner of such copyright, trademark or other proprietary right owned by a third party, and the burden of determining whether any material is protected by any such right is on you. You shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use any and all of Your Content. You represent and warrant that you have all rights, permissions and consents necessary (a) to make Your Content available on or through the Service, and (b) to grant Altirnao the limited rights to use Your Content set forth in these Terms.

You agree that Altirnao may use Your Content to provide the Service and its features, including by making it available for viewing, download and modification by other Users with access rights to Your Content. You hereby grant Altirnao a non-exclusive, perpetual, royalty-free, worldwide license (including the right to sublicense through multiple tiers) to access, use, reproduce, distribute, store, transmit, modify, adapt, reformat, publicly display, publicly perform and create derivative works of Your Content as required for the purpose of providing the Service to you.

You understand and agree that Altirnao does not have the ability to grant or revoke the Service's access to Customer's Google Apps domain data and files or other content and materials stored in Customer's Google Apps account. Therefore, You are solely responsible for granting the Service access to such Google Apps files and revoking such access when You cease use of the Service. Altirnao shall not be responsible and shall have no liability for any damages that result from Your failure to grant or revoke such access.

You understand and agree that Altirnao may, notwithstanding any provision of any separate nondisclosure agreement that may have been executed between You and Altirnao, distribute and disclose Your Content (a) to your Users, and (b) to Altirnao's service providers who act on Altirnao's behalf in providing the Service. Altirnao's use of any personally identifiable information you provide through the Service is governed by our Privacy Policy. Your use of the Service indicates your acceptance of the terms of our Privacy Policy. You can review the most recent version of our Privacy Policy at http://www .altirnao .com/pr ivacy-policy/ .

You hereby consent that, if You choose to become a paying customer of the Service, Altirnao may identify You as a Altirnao customer (using Your name and logo) and generally describe the products or services it provides to You in its promotional materials, presentations, and proposals to other current and prospective customers.

If you cancel your Service subscription, your information is no longer used and Altirnao will delete your Account and data associated with your Account within ninety (90) days of your cancellation. Please note, however, that some information like billing and subscription may remain with us for accounting and legal reasons.

Availability.

Altirnao will make the Service available to You in accordance with the Service Level Agreement available online at https://www.aodocs.com/sla (the **"SLA").** Altirnao does not make any representations or guarantees regarding uptime or availability of the Service unless specifically identified in the SLA. The Service may be unavailable at certain times as specified in the SLA, including during any unanticipated or unscheduled downtime or unavailability of all or any portion of the Service as a result of system failures or force majeure events.

Warranty Disclaimer

THE SERVICE IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE

OR NON-INFRINGEMENT. ALTIRNAO MAKES NO WARRANTY THAT (I) THE SERVICE IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS; (II) THE SERVICE WILL BE ERROR-FREE OR UNINTERRUPTED (INCLUDING, WITHOUT LIMITATION, INTERRUPTIONS THAT OCCUR IN THE CONTEXT OF REGULARLY SCHEDULED MAINTENANCE); (Ill) ANY INFORMATION OR ADVICE OBTAINED BY YOU IN CONNECTION WITH THE SERVICE WILL BE ACCURATE OR COMPLETE; OR (IV) THE RESULTS OF USING THE SERVICE WILL MEET YOUR REQUIREMENTS. SOME STATES DO NOT ALLOW EXCLUSION OF AN IMPLIED WARRANTY, SO THIS DISCLAIMER MAY NOT APPLY TO CUSTOMER.

Limitation of Liability

IN NO EVENT SHALL ALTIRNAO BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR OTHER LOSS OR DAMAGE WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, COMPUTER FAILURE, LOSS OF BUSINESS INFORMATION), ARISING OUT OF OR CAUSED BY YOUR USE OF OR INABILITY TO USE THE SERVICE, EVEN IF ALTIRNAO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY DISPUTE WITH ALTIRNAO RELATED TO ANY OF THE SERVICE SHALL BE TERMINATION OF SUCH SERVICE. IN NO EVENT SHALL ALTIRNAO'S ENTIRE LIABILITY TO YOU IN RESPECT OF ANY SERVICE, WHETHER DIRECT OR INDIRECT, EXCEED THE FEES PAID BY YOU TOWARDS SUCH SERVICE. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE LIMITATIONS OR EXCLUSIONS IN THIS PARAGRAPH MAY NOT APPLY TO CUSTOMER.

Other Terms

These Terms, their interpretation, performance or any breach thereof, will be construed in accordance with, and all questions with respect thereto will be determined by, the laws of the State of California. Both parties hereby irrevocably submit any disputes under these Terms to the jurisdiction of the courts located in the State of California.

Last Updated: February 11th, 2016

EAST\53456530.2

Published by Google Drive – Report Abuse – Updated automatically every 5 minutes

Channel Foundation Agreement
U.S. Public Sector

1. INTRODUCTION

1.1 This Channel Foundation Agreement ("Foundation Agreement") specifies the terms and conditions agreed between CA and the Ordering Activity, as defined in GSA Order ADM4800.2G and as revised from time to time ("End User" or "Customer") as a foundation for their relationship as further defined in the applicable Modules. Ordering Activity understands and agrees that Ordering Activity's right to use the CA Offerings, ordered by Ordering Activity and submitted to CA by an Authorized CA Partner, is subject to Ordering Activity's compliance with this Foundation Agreement and the relevant Module for such CA Offering. The Foundation Agreement and the Module(s) incorporated into the GSA Schedule contract for the CA Offering(s) purchased by Ordering Activity will govern orders from an Authorized CA Partner for Ordering Activity's acquisition of the CA Offering and such terms shall remain binding upon both Ordering Activity and CA for that CA Offering absent mutual written agreement to the contrary.

1.2 Modules to this Foundation Agreement include the Channel Software Module, , Channel SaaS Module, Channel Hardware Appliance Module, and Channel Education Module.

2. DEFINITION

2.1 "Agreement" means this Foundation Agreement, the applicable Module, and License Metric for the applicable CA Offering, and any document incorporated expressly therein or incorporating the foregoing by reference.

2.2 "Authorized CA Partner" means an entity having a valid, current authorization from CA to market, offer and resell to Ordering Activity the right to use the CA Offering. Ordering Activity may find information regarding authorized CA Partners here: www.ca.com/partners.

2.3 "CA Offering" means the individual offering (such as software, services, software as a service etc.) made available by CA as defined in the Module and/or, License Metric.

2.4 "Confidential Information" means any information, maintained in confidence by the disclosing Party, communicated in written or oral form, marked as proprietary, confidential or otherwise so identified, that is exempt from disclosure under the Freedom of Information Act (FOIA), 5.U.S.C. §552(b) under one or more exemptions to that Act, and/or any information that by its form, nature, content or mode of transmission would to a reasonable recipient be deemed confidential or proprietary, including, without limitation, CA Offerings, Documentation, and any benchmark data and results produced.

2.5 "Documentation" means the documentation, technical product specifications and/or user manuals, published by CA or any entity within CA group of companies (each a CA entity) that is made generally available with CA Offerings.

2.6 "License Metric" means the specific criteria for measuring the usage of the CA Offering (such as MIPS, CPUs, tiers, servers, or users).

2.7 "Module" means the additional terms and conditions applicable to the CA Offering.

2.8 "Parties" means individually and or collectively CA and or the Ordering Activity.

2.9 "Prime Contractor" means the entity contracting directly with the Ordering Activity, if other than an Authorized CA Partner.

2.10 "Term" means the period for which Ordering Activity is authorized to use the CA Offering as specified in CA's order with Ordering Activity's chosen Authorized CA Partner or the Prime Contractor.

3. ORDERING AND DELIVERY

3.1 This Agreement applies to each specific CA Offering purchased by Ordering Activity from an Authorized CA Partner or Prime Contractor. Use of the CA Offerings, or of this Agreement to procure CA Offerings, by Ordering Activity's Affiliates outside of the jurisdiction specified for Ordering Activity in the order between CA and the Authorized CA Partner or Prime Contractor is not permitted unless such Affiliate signs a participation agreement with CA to adopt and adhere to the terms of this Agreement.

3.2 CA will deliver or make available a CA Offering to Ordering Activity only upon, and in accordance with, CA's execution of an order with the Authorized CA Partner. Any terms that may appear on an Ordering Activity's purchase order (including without limitation pre-printed terms), or as part of Ordering Activity's order with an Authorized CA Partner or Prime Contractor, that conflict or vary from the terms and conditions of this Agreement shall not apply to CA and shall be deemed null and void unless otherwise required by law.

3.3 The CA Offering will be delivered by CA to Ordering Activity either by electronic delivery (ESD) or in tangible media in accordance with the terms of the GSA Schedule contract and the relevant purchase order. CA agrees to be responsible for all customs duties and clearances.

4. CONFIDENTIAL INFORMATION

4.1 The Parties agree that when receiving Confidential Information from the disclosing Party, that the receiving Party shall hold it in confidence and shall not disclose or use such information except as permitted under the Agreement. The receiving Party shall treat the disclosing Party's Confidential Information confidentially and in the same manner as it treats its own proprietary and/or confidential information, which shall not be less than a reasonable standard of care, and the receiving Party shall use Confidential Information only for the purposes described in the Agreement. Confidential Information may be disclosed to receiving Party's employees, agents, financial advisors, contractors and attorneys on a need-to know basis and the receiving Party shall ensure that such persons maintain such Confidential Information pursuant to the terms of the Agreement.

4.2 The receiving Party shall be permitted to disclose Confidential Information in connection with a judicial or administrative proceeding to the extent that such disclosure is required under applicable law or court order, provided that the receiving Party shall, where reasonably possible, give the disclosing Party prompt and timely written notice of any such proceeding and shall offer reasonable cooperation in any effort of the disclosing Party to obtain a protective order.

4.3 For the purposes of the Agreement, Confidential Information shall exclude: (i) information which the receiving Party has been authorized in writing by the disclosing Party to disclose without restriction; (ii) information which was rightfully in the receiving Party's possession or rightfully known to it prior to receipt of such information from the disclosing Party; (iii) information which was rightfully disclosed to the receiving Party by a third Party having proper possession of such information, without restriction; (iv) information which is part of or enters the public domain without any breach of the obligations of confidentiality by the receiving Party; and (v) information which is independently developed by the receiving Party without use or reference to the disclosing Party's Confidential Information.

4.4 Nothing in the Agreement will (i) preclude CA from using the ideas, concepts and know-how which are developed in the course of providing any CA Offerings to Ordering Activity or (ii) be deemed to limit CA's rights to provide similar CA Offerings to other customers. Ordering Activity agrees that CA may use any feedback provided by Ordering Activity related to any CA Offering for any CA business purpose, without requiring consent including reproduction and preparation of derivative works based upon such feedback, as well as distribution of such derivative works.

4.5 To the extent permitted by the Federal Records Act, the receiving Party agrees, upon request of the disclosing party, to return to the disclosing Party all Confidential Information in its possession or certify the destruction thereof.

4.6 For CA software (including code) and Documentation, and Ordering Activity's and/or CA's Confidential Information expressly designated in writing as perpetually confidential, the obligations of this section are perpetual and shall survive termination. For all other Confidential Information, the foregoing obligations shall extend for five (5) years from the date of initial disclosure.

5. FEES

5.1 The Parties acknowledge and agree that all terms governing the fees, payments, payment schedules, pricing and discounts for the applicable CA Offering procured by Ordering Activity under this Agreement are and shall be between solely Ordering Activity and their chosen Authorized CA Partner or Prime Contractor.

6. TITLE

6.1 CA retains all right, title, copyright, patent, trademark, trade secret and all other proprietary interests to all CA Offerings and any derivatives thereof. No title, copyright, patent, trademark, trade secret or other right of intellectual property not expressly granted under the Agreement is exchanged between the Parties.

7. WARRANTY

7.1 Each Party represents and warrants that it has the legal power to enter into the Agreement.

7.2 CA represents and warrants that it owns or otherwise has sufficient rights to grant Ordering Activity the rights defined in the Agreement.

8. INDEMNIFICATION

8.1 CA will indemnify any third party claims that Ordering Activity's use of the specific CA Offering licensed or purchased by Ordering Activity under this Agreement infringes any valid US patent or copyright within the jurisdictions where Ordering Activity is authorized to use the CA Offering at the time of delivery. CA may, at its option and expense: (i) procure for Ordering Activity the

right to continue to use the CA Offering; (ii) repair, modify or replace the CA Offering so that it is no longer infringing; or (iii) provide a pro-rated refund to the Authorized CA Partner of the fees paid for the CA Offering which gave rise to the indemnity calculated against the remainder of the Term from the date it is established that CA is notified of the third party claim. If the CA Offering is CA Software, and is licensed on a perpetual basis, an amortization schedule of three (3) years shall be used for the basis of the refund calculation.

8.2 CA shall have no liability: (i) in the event the allegation of infringement is a result of a modification of the CA Offering except a modification by CA, (ii) if the CA Offering is not being used in accordance with CA's specifications, related documentation and guidelines, (iii) if the alleged infringement would be avoided or otherwise eliminated by the use of a CA published update or patch, (iv) if the alleged infringement is a result of use of the CA Offerings in combination with any third party product, or (v) if the applicable fees due for the specific CA Offering have not been paid by Ordering Activity or Prime Contractor to its Authorized CA Partner. The indemnifications contained herein shall not apply and CA shall have no liability in relation to any CA Offering produced by CA at the specific direction of Ordering Activity. THE FOREGOING PROVISIONS STATE THE ENTIRE LIABILITY AND OBLIGATIONS OF CA REGARDING CLAIMS OF INFRINGEMENT, AND THE EXCLUSIVE REMEDY AVAILABLE TO ORDERING ACTIVITY WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS.

8.3 CA shall indemnify Ordering Activity against all damages, fees, (including reasonable attorney's fees) fines, judgments, costs and expenses finally awarded as a result of a third party action alleging a bodily injury or death which arises under the Agreement, provided that such liabilities are the proximate result of gross negligence or intentional tortuous conduct on the part of CA.

8.4 The above indemnities are contingent upon: (i) Ordering Activity providing prompt notice of any claim of infringement and assistance in the defense thereof, (ii) CA's right to consult with Ordering Activity at any time and to intervene in the proceedings through CA's chosen counsel at CA's expense, provided that Ordering Activity shall not have the right to settle any claim requiring CA to make a payment or to admit liability without CA's prior written agreement , and (iii) Ordering Activity not taking any actions or failing to take actions that hinder the defense or settlement process.

9. LIMITATION OF LIABILITY

EXCEPT IN THE CASE OF A BREACH OF TITLE, INFRINGMENT OF CA'S INTELLECTUAL PROPERTY RIGHTS OR CONFIDENTIALITY, OR OF THIRD PARTY CLAIMS ARISING UNDER THE INDEMNIFICATION SECTION, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER PARTY (INCLUDING ANY OF CA'S SUPPLIERS) SHALL BE LIABLE FOR A) ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING, BUT NOT NECESSARILY LIMITED TO, LOSS OF PROFIT, DAMAGES RELATING TO MONIES SAVED OR FEES GENERATED AND OR ANY LOSS OF DATA BY USE OF ANY CA OFFERING, REGARDLESS OF WHETHER A PARTY WAS APPRISED OF THE POTENTIAL FOR SUCH DAMAGES; AND B) IN NO EVENT WILL A PARTY'S LIABILITY, EXCEED THE FEES PAID AND OR OWED TO CA FOR THE THEN CURRENT INITIAL OR RENEWAL TERM FOR WHICH THE ORDERING ACTIVITY HAS PROCURED THE CA OFFERING OR AS FURTHER DEFINED IN THE MODULE. FURTHERMORE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CA SHALL NOT INCUR ANY LIABILITY FOR DEATH OR BODILY INJURY TO ANY THIRD PARTY UNLESS THE SAME ARISES FROM THE INTENTIONAL OR GROSSLY NEGLIGENT ACT(S) OF CA. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Agreement under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

10. TERM & TERMINATION

10.1 This Foundation Agreement shall continue in effect unless otherwise terminated in accordance with this section or as required pursuant to Federal Acquisition Regulation (FAR) 52.212-4 "Contract Terms and Conditions- Commercial Items" sections (l) "Termination for the Government's Convenience" and (m) "Termination for Cause."

10.2 In the event Ordering Activity elects to terminate an order for its convenience prior to the expiration of the then current term, and such order includes licenses for CA Software, Ordering Activity shall also, within a reasonable period of time, delete all copies of such software from its systems, including copies stored for archival purposes and either destroy or return them to CA. The foregoing shall not apply, however, where such licenses were perpetual and Ordering Activity, at the time of such termination, has paid all associated perpetual license fees.

10.3 Termination does not release either Party from any liability which, at the time of such termination, had already accrued to the other Party or which is attributable to a period prior to such termination, nor preclude either Party from pursuing any rights or remedies it may have under law or in equity with respect to any breach of this Foundation Agreement or the Agreement.

11. DISPUTE RESOLUTION

11.1 Prior to the initiation of formal dispute resolution procedures regarding any dispute, controversy, or claim arising out of the Agreement or interpretation thereof (a "Dispute"), the Parties shall first meet as often, and for such duration and as promptly as the Parties reasonably deem necessary to discuss the Dispute and negotiate in good faith in an effort to resolve it.

11.2 The provisions of paragraph 11.1 will not be construed to prevent a Party from instituting formal proceedings to the extent necessary to avoid the expiration of any applicable limitations period or to pursue equitable rights or injunctive remedies deemed reasonable necessary to protect its interests.

11.3 Disputes relating to the payments of fees, any third party products or services or otherwise relating to the terms and conditions of an order between an Authorized CA Partner and Ordering Activity, shall be between Ordering Activity and such Authorized CA Partner, or if applicable, between Ordering Activity and Prime Contractor, and Ordering Activity agrees that it shall have no right of contribution or other claim from or against CA by reason thereof.

12. GENERAL TERMS

12.1 **Amendments**. The terms of the Agreement may only be amended by mutual written agreement of the Parties.

12.2 **Force Majeure**. Except for payment obligations and obligations pertaining to non-disclosure, notwithstanding any contrary provision in the Agreement, neither Party will be liable for any action taken, or any failure to take any action required to be taken, in the event and to the extent that the taking of such action or such failure arises out of causes beyond a Party's control, including, without limitation, war, civil commotion, act of God, strike or other stoppage (whether partial or total) of labor, any law, decree, regulation or order of any government or governmental body (including any court or tribunal).

12.3 **Order of Precedence**. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) the relevant Module and(3) this Channel Foundation Agreement. Notwithstanding this Order of Precedence, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

12.4 **Ordering Activity Data**. If Ordering Activity transfers any personal data to CA as a requirement pursuant to any CA Offering, then Ordering Activity represents that (i) it is duly authorized to provide personal data to CA and it does so lawfully in compliance with relevant legislation, (ii) CA and any entity within the CA group of companies (each a "CA entity") or its subcontractors can process such data for the purposes of performing its obligations and (iii) CA may disclose such data to any CA entity and its subcontractors for this purpose and may transfer such data to countries outside of the country of origin. CA, Inc. is Safe Harbour certified and the CA Entities have committed to comply with relevant data protection/privacy legislation.

12.5 **Import Export**. Ordering Activity agrees that CA Offerings, Documentation, and or Confidential Information is subject to export controls of the United States of America and import controls of any other country in which such information may be used. Ordering Activity agrees to export, re-export or import such information only in compliance with such laws and controls.

12.6 **Announcements**. Neither Party may issue press releases relating to the Agreement without approving the content with the other Party. Either Party may include the name and logo of the other Party in lists of customers or vendors in accordance with the other Party's standard guidelines.

12.7 **Counterparts**. This Foundation Agreement and any Module, as applicable, may be signed in any number of counterparts by the Parties and each part shall be considered part of the whole and valid, legally binding document.

12.8 **Notice**. All notices hereunder shall be delivered to the other Party identified in the Agreement either personally, via certified mail, facsimile or overnight courier. If delivered personally, notice shall be deemed effective when delivered; if delivered via facsimile, notice shall be deemed effective upon electronic confirmation; and if delivered via certified mail or overnight courier, notice shall be deemed effective upon confirmation of delivery.

12.9 **Headings**. The section headings used herein are for information purposes only and shall not affect the interpretation of any provision of this Agreement.

12.10 **Validity**. In the event any term or provision of the Agreement shall be held to be invalid, the same shall not affect in any respect whatsoever the validity of the remainder of the Agreement.

12.11 **Third Parties**. This Agreement shall not create any rights in favor of, or any obligations owed by, any third party unless otherwise expressly defined in any Module. The Parties agree that any action arising from this Agreement shall solely be brought by Ordering Activity, the U.S. Government, or CA, unless otherwise permitted by law.

12.12 **Choice of Law**. To the extent that federal law is not dispositive of a dispute hereunder, the laws of the State of New York (excluding its conflict of laws provisions) shall govern the construction and enforceability of the Agreement.

12.13 **Survival**. Sections pertaining to Confidentiality, Title, Limitation of Liability, Termination, and Import Export shall survive termination of this Foundation Agreement.

12.14 **Entire Agreement**. The Agreement and all documents incorporated by reference therein shall comprise the entire agreement as pertaining to the subject matter thereof and all other prior representations, proposals, and other such information exchanged by the Parties concerning the subject matter is superseded in their entirety by the Agreement.

Channel SaaS Module

U.S. Public Sector

1. INTRODUCTION

1.1. This Module for Software as a Service ("SaaS Module") specifies terms and conditions which apply to Software as a Service that CA will provide to Ordering Activity.

1.2. This SaaS Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this SaaS Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Ordering Activity Data" means information stored in the SaaS database.

2.2. "Force Majeure Event" means an event of Force Majeure as defined in the Foundation Agreement and/or delays caused by an internet service provider or hosting facility that results in data center outages resulting from causes not within CA's control.

2.3. "ISO 27001" means an Information Security Management System standard published by the International Organization for Standardization (ISO). This particular standard specifies a management system that is intended to bring information security under explicit management control and mandates specific requirements when this standard is met.

2.4. "Production" means the "live" environment of SaaS provided to process data on a real-time basis.

2.5. "Production Availability" means, for purposes of measuring the Service Level, the aggregate number of minutes during the month in which the SaaS is available for Production access and use by Ordering Activity.

2.6. "SaaS" means the online version of the CA Software specified in the Authorized CA Partner's order with CA for access to and usage by its customers via a website(s) environment.

2.7. "SAS 70 Type II" means the standards used by an independent auditor that employs procedures, policies and controls of SAS 70 Type I to verify and validate that the organization is following those procedures regarding control objectives, activities and control over information technology, and related processes.

2.8. "SaaS Support" means support of the underlying CA software so it operates materially in accordance with the Documentation.

2.9. "Sandbox" means a development or test environment that is not Production.

2.10. "Scheduled Downtime" means planned downtime of SaaS availability where CA provides notice to Ordering Activity at least 72 hours in advance.

2.11. "Service Level" means as described in the section entitled: Service Level Commitments.

2.12. "Subscription Term" means the period of the Ordering Activity's subscription to the SaaS as specified in the Authorized CA Partner's order with CA.

2.13. "Users" means the number of individuals authorized to access and use of SaaS by Ordering Activity and who have been provided user identifications and passwords by Ordering Activity (or by CA at Ordering Activity's request), measured by CA on an aggregate monthly basis by the amount of User Logins. Users may include Ordering Activity and Affiliate's employees and independent contractors that agree to be bound by terms and conditions no less restrictive than those contained herein and are acting on behalf of Ordering Activity and not a third party.

2.14. "User Logins" means the initial and standard login screen where a User is required to enter its user ID and the password.

3. SAAS OFFERING

3.1. CA shall provide SaaS to Ordering Activity during the Subscription Term directly or through a third party SaaS provider in accordance with the terms of the Agreement.

3.2. CA hereby provides Ordering Activity a non-transferable and non-exclusive right to access and use SaaS for the sole purpose of supporting its internal business use. A new User may replace a former User who no longer requires access to, or use of, the SaaS. Users may be Ordering Activity employees, Ordering Activity third party consultants, contractors or agents, which third parties may

access and use the SaaS solely for the benefit of Ordering Activity's internal business purposes in accordance with the provisions of this Agreement.

3.3. Ordering Activity acknowledges and agrees that in order for CA to effectively provide SaaS, Ordering Activity may be required to provide necessary information and shall not delay, prevent or interfere with CA's provision of SaaS.

4. FEES & RENEWAL

4.1. Ordering Activity may access SaaS for solely the number and type of Users specified in the Authorized CA Partner's order with CA. Additional Users, or an additional SaaS offering, if available, shall require Ordering Activity to procure with CA or an Authorized CA Partner (whether directly or through a Prime Contractor) for such users or offering. Unless otherwise agreed by CA, (i) additional Users may be purchased only in increments of 50 Users; and (ii) such additional User subscriptions shall be coterminous with the expiration of the Subscription Term.

4.2. CA may with notice prior to any renewal, replace the Ordering Activity ordered SaaS with replacement, underlying software that is generally available to customers with alternative, materially similar, functionality.

4.3. The fees for SaaS subscription are not contingent upon the delivery of any future functionality or features of the CA Software.

5. ORDERING ACTIVITY DATA

5.1. Ordering Activity exclusively owns all rights, title and interest in and to all Ordering Activity Data. Ordering Activity Data shall be considered to be Confidential Information under the Agreement. CA shall not access Ordering Activity's User accounts, or Ordering Activity Data, except (i) in the course of data center business operations if required, (ii) in response to SaaS or technical issues or (iii) at Ordering Activity's specific request as reasonably required in the provision of SaaS. CA will segregate Ordering Activity's Data from other customers' data.

5.2. CA operates and maintains a disaster recovery procedure. In case of a Force Majeure Event, Ordering Activity acknowledges and agrees that Ordering Activity Data may not be recoverable and accepts responsibility for re-entry of such data.

5.3. Ordering Activity Data will be returned to the Ordering Activity at the end of the Subscription Term or at the termination of the SaaS subscription in the manner described in the SaaS Documentation.

6. SECURITY

6.1. CA shall adhere to SAS 70 Type II audit compliance criteria and data security procedures which meet ISO 27001 status during the Subscription Term.

6.2. CA shall comply with CA's security policy and procedures, which policies and procedures are designed to provide and maintain commercially reasonable safeguards against the destruction, loss or alteration of, or unauthorized access to or use of the Ordering Activity Data in CA's possession or control and which safeguards are, at a minimum, no less rigorous than those maintained by CA for its own information of a similar nature.

6.3. Ordering Activity Data shall be stored pursuant to CA's data security procedures, which shall be provided to Ordering Activity upon request. Except as required herein, CA will not be responsible for any unauthorized access to, or alteration, theft or destruction of Ordering Activity Data, unless caused as a result of CA's negligence or intentional misconduct, in which case restoring or recovery of Ordering Activity Data shall be limited to the most recent back-up of Ordering Activity Data. CA is not responsible for loss of Ordering Activity Data arising from Ordering Activity's: (i) transmission of data in contravention of the User Guide; or (ii) failure to act on any CA provided communication.

6.4. CA shall comply with the applicable EU member states' implementation of the Directive 95/46/EC ("Directive") governing the processing of personal data as defined specifically in the Directive and CA, Inc. is Safe Harbour certified.

6.5. Ordering Activity or an independent third party may audit CA's operations within the applicable data center to verify CA's compliance with the security and technical provisions defined in this Module. The audit may take place, no more than once annually, upon thirty (30) days prior written notice subject to Ordering Activity or its independent third party having executed a CA confidentiality agreement and stating the purpose and scope of the request. Such audit shall be conducted during normal business hours in a manner that does not disrupt business operations.

7. INITIATION AND SUPPORT PROCESSES

7.1. The following processes apply to the SaaS:

i. CA will send an email to Ordering Activity's technical contact identified in the Authorized CA Partner's order with CA setting out the SaaS URL(s) and other information necessary for initial use of the SaaS. Ordering Activity shall provide information as requested within 7 days of receiving the email.

ii. Customer will utilize the CA Support website, or other site or notification mechanism as CA may designate from time to time, to notify CA of SaaS availability issues, request other in-scope technical support assistance, or for Customer's to provide feedback or approvals on requests as applicable.

8. SAAS SUPPORT

8.1. The Ordering Activity shall be provided with SaaS Support during the Subscription Term.

8.2. For any SaaS Support requests, Ordering Activity should be prepared to provide to SaaS Support personnel, all pertinent information, in English, including but not limited to, Ordering Activity number or site identification number, incident severity, SaaS/software name, area of SaaS (Production or Sandbox), incident description, and a technical contact familiar with Ordering Activity's environment or the problem to be solved. Ordering Activity must use reasonable efforts to communicate with CA in order to verify the existence of the problem and provide information about the conditions under which the problem could be duplicated.

8.3. Upon receiving Ordering Activity's technical contact information, SaaS Support will be provided in a timely and professional manner by qualified support engineers as defined below:

i. Access to CA help desk and the ability to open and manage support incidents via CA support online or by telephone.

ii. Production environment support: 24x7 for severity 1 incidents; normal business hours for severities 2-4.

iii. Sandbox environment support: Normal business hours for incidents of all severities.

iv. Access to CA support website (currently: http://support.ca.com) for 24x7x365 online support and access to CA software product and documentation, global user communities and regional user groups, FAQs, samples, webcast recordings and demos, usage tips, technical updates and HYPER notifications, as such are made available by CA.

v. Interactive remote diagnostic support allowing CA support engineers to troubleshoot an incident securely through a real-time browser-based remote control feature.

vi. Additional support such as file storage, point in time backup, periodic file refresh and basic reporting may be available at CA's discretion according to the SaaS provided.

Any additional support requirements are only by prior written agreement with CA.

8.4. In order to respond to an issue raised through SaaS Support, CA may request Ordering Activity to upgrade to appropriate operating systems and or third party applications as required in order to properly operate and access the SaaS offering. Any such upgrades or installations shall be at the Ordering Activity's sole option and discretion. The costs associated with any upgrades required and any such installations are not included as SaaS Support and all such costs shall be the responsibility of the Ordering Activity.

9. ORDERING ACTIVITY RESPONSIBILITIES

9.1. Ordering Activity is responsible for all activities that occur in, or are related to, User accounts including the data, information stored or transmitted when accessing SaaS.

9.2. Because Ordering Activity may integrate or utilize third party links to other software, hardware or other service which are associated with, or otherwise available through SaaS, Ordering Activity agrees that it and its Users shall use such third party links in their sole discretion. CA shall have no responsibility or liability with respect to such third party links used by Ordering Activity's or Users' or for any act or omission of any such third party provider.

9.3. Ordering Activity shall not: (i) make SaaS available to any third party not authorized, other than to Users or as otherwise contemplated by this Agreement; (ii) send or store code that can harm or result in damage to the SaaS offering (including but not limited to malicious code and malware); (iii) wilfully interfere with or disrupt the integrity of SaaS or the data contained therein; (iv) attempt to gain unauthorized access to the SaaS or its related system or networks; (v) use SaaS to provide services to external end users and or to process data other than Ordering Activity's as an outsourcer, service bureau or consultant without written permission provided by CA.

10. WARRANTY

10.1. CA warrants that (i) SaaS shall perform materially in accordance with the applicable SaaS Documentation and (ii) that SaaS will be available online according to the performance levels described in the Service Levels defined in this SaaS Module.

10.2. EXCEPT AS EXPRESSLY SET FORTH ABOVE, TO THE EXTENT PERMITTED BY LAW, NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THIRD PARTY WARRANTIES, IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY OR SATISFACTORY QUALITY, OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA AND CA MAKES NO WARRANTIES HEREUNDER WITH RESPECT TO ANY HARDWARE EQUIPMENT OR THIRD PARTY SOFTWARE WHICH CA MAY USE TO PROVIDE THE SAAS.

10.3. Ordering Activity warrants that (i) it has the right to transmit any data or information as may be required for the purposes of accessing SaaS (ii) it will ensure compliance to the Agreement by itself and its Users and (iii) it is responsible for all activities that occur in User accounts, (iv) it shall not misuse SaaS through sending spam or otherwise duplicative or unsolicited messages or store infringing, obscene, threatening, or otherwise unlawful material that is harmful to children or violates third party privacy rights.

11. WARRANTY REMEDY

11.1. In the event of a breach of the Warranty by CA, CA may in consultation with Ordering Activity (i) use reasonable efforts consistent with industry standards to cure the defect as defined in CA Support process outlined in this SaaS Module and or (ii) Ordering Activity may exercise its rights to termination as defined under the Service Level Commitment section below and qualify for a refund as defined therein and or (iii) mutually agree with Ordering Activity to terminate the subscription and provide a pro-rata refund to the Authorized CA Partner calculated on the number of months left remaining on the Subscription Term. Warranty remedies are conditioned upon (i) any error or defect complained of is reasonably reproducible by CA, (ii) the breach is not attributable in whole or in part to any non-CA product(s) or service(s).

12. SERVICE LEVEL COMMITTMENT

12.1. Service Levels: The following Service Levels will apply to the applicable SaaS offering during the applicable Subscription Term:

i. Production Availability of SaaS 99.5% on a monthly basis. If Production Availability falls below 99%, it shall be considered a minor failure; and if Production Availability falls below 98%, it shall be considered a major failure.

12.2. Ordering Activity will be provided monthly electronic reports regarding Service Levels and follow the procedure set out below:

i. CA will investigate missed Service Levels through determining the root cause of the issue then using commercially reasonable efforts to correct the issue and advising Ordering Activity as reasonably requested by Ordering Activity of the status of efforts being undertaken with respect to the issue;

ii. Provide Ordering Activity reasonable evidence to Ordering Activity that the cause of the issue is being corrected or will be corrected and

iii. In the event of a minor failure, Ordering Activity is entitled to 2 additional days of the applicable SaaS offering at no additional charge. In the event of a major failure, Ordering Activity is entitled to 5 additional days of the applicable SaaS offering at no additional charge.

12.3. Pursuant to FAR 52.212-4(l), Ordering Activity may terminate for convenience its subscription to SaaS without incurring any additional charges or termination fees. In the event of such termination for convenience CA shall refund to the CA Authorized Partner that portion of the fees paid which have not yet been applied towards SaaS as of the effective date of termination. Any such refund herein shall be Ordering Activity's sole and exclusive remedy under this SaaS Module with respect to CA only and CA shall have no further liability arising out of the applicable SaaS subscription, and shall not impact termination of any other Module or the Foundation Agreement. This section does not limit the rights or remedies of the Ordering Activity under FAR 52.212-4(m), Termination for cause.The following events shall be excluded from the calculation of any Service Level failures: (i) Force Majeure Event; (ii) outages due to Scheduled Downtime such as upgrading data center infrastructure; (iii) outages based on Ordering Activity networks or domain name server issues; (iv) Ordering Activity's configuration, scripting, coding; (v) internet outages; (vi) Ordering Activity outages requested by Ordering Activity (vii) Ordering Activity changes to its environment which hinder SaaS production and (viii) inability for Ordering Activity to log in due to use of Lightweight Directory Access Protocol (LDAP) to control authentication.

13. NIMSOFT SaaS

13.1. The following sections of this Module are not applicable to Nimsoft Saas transactions:

i. 2.2;

ii. 2.3;

iii. 2.7;

iv. 5.2;

v. 6.1;

vi. 6.5 and

vii. 12.2;

13.2. The following sections of this Module are modified or added as follows for Nimsoft SaaS (On-Demand) transactions to the extent consistent with U.S. Federal law:

i. Section 7.1 ii: "Ordering Activity will utilize the **Nimsoft** CA Support website, or other site or notification mechanism as CA may designate from time to time, to notify CA of SaaS availability issues, request other in-scope technical support assistance, or for Ordering Activity to provide feedback or approvals on requests as applicable."

ii. Section 8.1: "The Ordering Activity shall be provided with SaaS Support pursuant ot the terms of http://www.nimsoft.com/content/dam/nimsoft/documents/un-secure/agreements/nimsoft-us-support-agreement.pdf during the Subscription term."

iii. Section 10.1: "CA warrants that (i) SaaS shall perform materially in accordance with the applicable SaaS Documentation for a period of 60 days from the commencement of the Term and (ii) that SaaS will be available online according to the performance levels described in the Service Levels defined in this SaaS Module.

iv. Add the following as Section 15:

"15. **REPORTING AND AUDIT**

Reports. Ordering Activity agrees to prepare and submit monthly reports to the Authorized CA Partner and CA that shall include, without limitation, information detailing the use of SaaS pursuant to the license metrics applicable to SaaS ("Report"). Ordering Activity shall submit each Report to the Authorized CA Partner and CA on the fifteenth day of each calendar month.

Overage. If the Report shows the Ordering Activity has exceeded the Authorized Use Limitation at any time during a month, such Report shall constitute a basis for a claim to the relevant Contracting Officer pursuant to the Contract Disputes Act and FAR 52.233-1. In no event may the SaaS quantity be lowered below the original numberordered.

14. **GENERAL TERMS**.

14.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel SaaS Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

Channel Hardware Appliance Module
U.S. Public Sector

1. INTRODUCTION

1.1. This Module for the Hardware Appliance ("Hardware Appliance Module") specifies terms and conditions which apply to the Hardware Appliance which CA will provide to Ordering Activity.

1.2. This Hardware Appliance Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Hardware Appliance Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Hardware" means a single CA-supplied third party physical server or device.

2.2. "Hardware Appliance" means Hardware that is bundled with and operates the CA Software licensed by Ordering Activity and pre-installed on the Hardware.

3. APPLIANCE OFFERING

3.1. CA shall provide the Hardware Appliance specified in the Authorized CA Partner's order with CA.

3.2. The terms for license and support for the underlying CA Software is covered separately under the Software Module.

4. FEES

4.1. Ordering Activity may order Hardware Appliance with, and pay the associated fees and other charges to an Authorized CA Partner or Prime Contractor. CA will deliver to Ordering Activity the Hardware Appliance specified in the Authorized CA Partner's order with CA.

4.2. Upon CA's receipt of payment from the Authorized CA Partner, Ordering Activity will own the Hardware free of any liens or encumbrances.

5. WARRANTY

5.1. Upon the purchase of a Hardware Appliance, CA will pass through to the Ordering Activity the applicable Hardware warranty. Such warranty will be provided for a period of twelve (12) months or more depending on the type of Hardware Appliance purchased. A copy of the applicable third party support warranty coverage is available under the "Get Support" section of CA's Support website located at https://support.ca.com.

6. WARRANTY REMEDY

6.1. To address a warranty issue on the Hardware, CA will provide Ordering Activity telephone assistance to access the third party Hardware support to address support issues with the Hardware.

6.2. Except for procuring third party warranty coverage for the Hardware as described above, the Hardware is provided on an "AS IS" basis and CA makes no warranties, and disclaims any and all express or implied warranties (including but not limited to warranties of merchantability or satisfactory quality or fitness for a particular purpose), with respect to the Hardware. None of the warranties specified in the Foundation Agreement or any other agreement shall apply to the Hardware.

7. ORDERING ACTIVITY REQUIREMENTS

7.1. Ordering Activity is solely responsible for use of the Hardware, including assuring proper supported environment configuration, CA software installation, and operating methods in accordance with the Hardware specifications and Documentation.

7.2. CA will not support modifications to the Hardware nor will it support the Hardware if Ordering Activity fails to comply with the terms of the Agreement to the extent such failure causes the Hardware's failure to perform in substantial accordance with the applicable Hardware documentation.

7.3. CA shall have no obligation to replace the Hardware, or provide additional hardware, in cases where future Versions or Releases (as such terms are defined in the Software Module) of the CA Software require an upgrade of or addition to such Hardware.

8. GENERAL TERMS

8.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel Hardware Appliance Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase

order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

Channel Education Module
U.S. Public Sector

1. INTRODUCTION

1.1. This Module for Education ("Education Module") specifies terms and conditions which apply to Education that CA will provide to Ordering Activity.

1.2. This Education Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Education Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Attendees" mean the participants authorized by Ordering Activity to attend or participate in the Education offerings as indicated in the Transaction Document.

2.2. "Course Materials" means any Education content provided to Ordering Activity in any media form pursuant to a Transaction Document, including without limitation, all publications, courseware, training manuals and materials, user guides, web portals, or virtual labs provided by CA or a CA subcontractor.

2.3. "Education" means any standard or customized education offerings, training or instruction, or related services, provided by CA or a CA subcontractor in any format or location, including without limitation, (i) instructor led training, including at CA or Ordering Activity site(s), (ii) virtual training, including online classes, courses, or course catalogues and/or (iii) class room training or testing, at a CA or third party training facility.

3. EDUCATION OFFERING

3.1. CA shall provide the Education as specified in the Authorized CA Partner's order with CA.

3.2. CA may require the registration or pre-registration of Attendees in order to attend or access the applicable Education. Ordering Activity acknowledges that CA reserves the right to refuse entry or access to any individual that cannot authenticate their registration or authorization for such Education.

4. FEES AND CANCELLATION

4.1. The Parties acknowlede and agree that all terms governing the fees, payments, payment schedules, pricing and discounts for the applicable CA Offering procured by Ordering Activity under this Agreement are and shall be between solely Ordering Activity and their chosen Authorized CA Partner or Prime Contractor.

4.2. If CA cancels a class due to unforeseen circumstances, or low enrollment, CA will provide as much advance notice as possible but no less than ten (10) business days prior to the class in which case Ordering Activity may reschedule the class to an alternative time.

4.3. Cancellation in writing by Ordering Activity must be provided at least ten (10) business days prior to the class. If such notice is not given CA may charge Authorized CA Partner up to 100% of the fees for the class. If fees are pre-paid, no refund will be provided to the Authorized CA Partner

4.4. Neither party shall be liable for any travel related fees or expenses incurred by the other party in relation to Education which such party has properly cancelled in compliance with this section.

5. INTELLECTUAL PROPERTY RIGHTS

5.1. CA grants to Ordering Activity, a non-exclusive, non-transferable license to use the Course Materials for the internal use of the Ordering Activity, but limited to the specific Attendees and subject to terms of the Agreement. Ordering Activity shall be responsible for all use of the Education and Course Materials by its Attendees.

6. WARRANTY

6.1. If CA provides an instructor, the delivery of the Course Offering shall be provided in a professional, workman-like manner.

6.2. EXCEPT AS SET FORTH IN THIS SECTION, NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THIRD PARTY WARRANTIES, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR SUITABILITY AND/OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA.

7. WARRANTY REMEDY

7.1. In the event of a breach of the Warranty section, Ordering Activity's remedy shall be, at CA's discretion and in consultation with Ordering Activity, to re-perform the Education at no additional charge to the Ordering Activity. These remedies are contingent upon the alleged breach not resulting from Ordering Activity's failure to abide by its obligations or to conform to the Course Materials.

8. GENERAL TERMS

Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel Education Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

1. INTRODUCTION

1.1. This Module for CA Software ("Software Module") specifies terms and conditions which apply to CA Software that CA will license to Ordering Activity and the Support that applies.

1.2. This Software Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Software Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITION

2.1. "Access" means use of CA Software remotely by an Authorized End User.

2.2. "Authorized End Users" means Ordering Activity as well as its employees and support contractors (but excluding any outsourcer, facilities management providers, managed service provider, or application service provider) that are bound by terms and conditions no less restrictive than those contained herein and are acting on behalf of Ordering Activity and not a third party.

2.3. "Authorized Use Limitation" means the quantity of the CA Software authorized by CA in accordance with the License Metric specified in the order between CA and the Authorized CA Partner.

2.4. "CA Software" means the computer software programs, either provided individually or packaged as a software appliance, made generally available and licensed to a Ordering Activity under this Module, including all Versions, Releases, provided as part of Support if applicable.

2.5. "Distributed" means the CA Software designated as distributed that is generally used for indepedent usage across individuals systems or hardware based on the Licensed Metric in a decentralized form of computing.

2.6. "Mainframe" means CA Software designated as mainframe that is generally used for a large capacity processor that provides links to users through less powerful devices such as workstations or terminals based on the Licensed Metric in a centralized form of computing.

2.7. "Maintenance" means the provision of new Releases made available while on active Support or new Versions if applicable to the generally available CA Software licensed by Ordering Activity.

2.8. "Perpetual License" means a license to use CA Software for an indefinite period subject to compliance with the Agreement.

2.9. "Release" means a general available release of a CA software product, which may contain minor new software product functionality, code, or compatibility and incorporates all previous fixes (if any exist) since the last Version. Typically, a Release requires a new installation, rather than an overlay to the already installed software. Unless otherwise specified by CA for a particular product, a Release is tied to the preceding Version and is typically designated by a number to the right of the decimal point such as 1.1, 1.2, 1.3, etc.

2.10. "Subscription" or "UMF" (Usage and Maintenance Fee) license means a license to use CA Software for a specific period of time which shall include Support unless otherwise specified by CA in its order with the Authorized CA Partner.

2.11. "Support" means the provision of technical support and Maintenance provided for a particular CA Software as specified in the Authorized CA Partner's order with CA.

2.12. "Territory" is the location where Ordering Activity is authorized to install the CA Software as specified in the Authorized CA Partner's order with CA or the Prime Contractor.

2.13. "Version" means a release of a CA Software Product that contains major changes in software product functionality, code, or compatibility and incorporates the previous release (if one has occurred), fixes and service Packs (if they have occurred). Typically, a Version requires a new installation, rather than an overlay to the already installed software. Unless otherwise specified by CA for a particular product, a Version is designated by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc.

3. SOFTWARE OFFERING & OBLIGATIONS

3.1. CA grants the Ordering Activity a limited, non-exclusive, non-transferable license, for the Term:

3.1.1. install and deploy the CA Software in the Territory up to the Authorised Use Limitation.

3.1.2. permit its Authorized End Users Access to the CA Software for Ordering Activity's and Affiliates' internal business wherever located. Ordering Activity hereby expressly agrees that a breach by an Authorized End User of the Agreement shall be considered to be a breach by and the responsibility of the Ordering Activity.

3.1.3. make a reasonable number of copies of the CA Software for disaster recovery "cold standby", backup and archival purposes. Use of such copies is limited to testing Ordering Activity's disaster recovery procedures and effectiveness and as is necessary during any reasonable period subsequent to the occurrence of an actual disaster during which Ordering Activity cannot operate the CA Software.

3.1.4. relocate CA Software to a new Ordering Activity location within the Territory upon prior written notice.

3.2. The specifications and specified operating environment information of the CA Software may be found in the Documentation accompanying the CA Software, if available (e.g., a user manual, user guide, or readme.txt or notice.txt file).

3.3. Upon request by CA, Ordering Activity agrees to provide records reasonably requested by CA to verify its compliance with the Authorized Use Limitation during the period in which Ordering Activity is licensed to use the CA Software and for a period of twelve (12) months after expiration including certified copies of statements or records as applicable. Such reports will be based on the License Metric for the CA Software ordered for Customer by CA.

3.4. The grant of license is contingent upon Ordering Activity's compliance with the following obligations set out under this provision: Ordering Activity agrees, that it shall not: (i) access or use any portion of the CA Software not expressly authorized by CA or the Documentation of the CA Software; (ii) cause or permit de-compilation, reverse engineering, or otherwise translate all or any portion of the CA Software; (iii) modify, unbundle, or create derivative works of the CA Software and/or Documentation; (iv) rent, sell, lease, assign, transfer or sublicense the CA Software or use the CA Software to provide hosting, service bureau, on demand or outsourcing services for the benefit of a third party; (v) remove any proprietary notices, labels, or marks on or in any copy of the CA Software or Documentation; (vi) use the CA Software beyond the Authorized Use Limitation.

3.5. CA reserves the right, on reasonable notice to the Ordering Activity and subject to any security measures the Ordering Activity deems appropriate, to conduct an audit remotely or onsite of Ordering Activity and/or its Affiliates facilities to verify Ordering Activity's compliance with the terms of the Agreement. CA agrees that such audit shall be conducted during regular business hours at Ordering Activity's offices and CA shall endeavor to conduct such audit so as not to interfere unreasonably with Ordering Activity's activities and/or use an independent third party to conduct the audit subject to terms of non-disclosure if required.

3.6. All rights not specifically granted hereunder are expressly reserved.

4. SUPPORT OFFERING

4.1. If Support is purchased by Ordering Activity, CA will provide Ordering Activity with technical support for the CA Software, according to the Support specified in the Authorized CA Partner's order with CA, to operate according to the Documentation, help desk support and Maintenance for the CA Software based on Support guidelines as described on http://www.support.ca.com.

4.2. In order to initiate an issue, Ordering Activity will provide CA sufficient information so that CA can provide assistance to Ordering Activity in a timely manner.

4.3. CA will provide a minimum of twelve months prior written notice to Ordering Activity if CA ceases to provide new Versions or Releases for a CA Software product.

4.4. CA will renew Support for Ordering Activity's use of the CA Software upon its acceptance of an order with an Authorized CA Partner for such Support.

5. THIRD PARTY TERMS

The CA Software may contain third-party software components. Ordering Activities are advised to review any additional terms, notices, and/or information applicable to third-party software components, which are available at https://support.ca.com/prodinfo/tpterms.

6. PERFORMANCE WARRANTY

6.1. For Distributed Software. CA warrants that the CA Software will operate materially in accordance with the applicable specifications set forth within the Documentation for a period of ninety (90) days after delivery of the CA Software to Ordering Activity subject to Ordering Activity's compliance with the Agreement.

6.2. For Mainframe Software. CA warrants that the Mainframe Software will operate materially in accordance with the applicable specifications set forth within the Documentation for the Term, subject to Ordering Activity's compliance with the Agreement.

7. PERFORMANCE WARRANTY REMEDY

7.1. If CA has breached either warranty set forth in the section entitled: Performance Warranty, Ordering Activity's remedy is for CA to, in consultation with Ordering Activity, to either (i) use reasonable efforts consistent with industry standards to cure the defect, or (ii) replace the CA Software(s) with one that materially complies with the Documentation, or (iii) mutually agree to terminate the license

and provide a pro-rata refund to the Authorized CA Partner of the license fees paid and or Support fees. If option (iii) applies, the pro-rata refund shall be calculated on the number of months left remaining on the Term of the applicable Transaction Document or if the CA Software is licensed under a Perpetual License, using (only for purposes of a refund calculation) an amortization schedule of three (3) years.

7.2. Warranty remedies are conditioned upon (i) any error or defect complained of is reasonably reproducible by CA, (ii) the CA Software is not modified and is being used in accordance with CA Documentation, and (iii) the breach is not attributable in whole or in part to any non-CA product(s) or service(s).

7.3. **THE ABOVE WARRANTIES ARE THE SOLE WARRANTIES PROVIDED BY CA. NO OTHER WARRANTIES, INCLUDING THAT THE CA SOFTWARE IS ERROR FREE, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR SUITABILITY AND/OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA.**

8. ACCEPTANCE

8.1 All CA Software is deemed accepted upon issuance of an order to CA from CA Authorized Partner.

9. VIRTUALIZATION

When CA Software is used on multiple machines (physical and "virtual"), each such use of the CA Software shall be counted for the purposes of determining the Authorized Use Limitation for that CA Software. A "virtual" PC or server environment is created where Virtual Machine Technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously.

10. NEW PRODUCT LANGUAGE AND DISTRIBUTED CA SOFTWARE EXCLUSION

10.1 In addition to and separate from unspecified upgrades and enhancements to be provided as maintenance under the initial Term specified in the order with Authorized CA Partner (together with any extension(s) or renewal(s) thereof, the "Term" for purposes of this section), in the event CA develops a new release of a mainframe CA Software that it designates and makes generally available as a new product (typically containing new functions in addition to or different from existing functionality (a "New Product"), then upon CA's receipt of Ordering Activity's written request and without additional charge, such currently unspecified mainframe New Product shall be made available for use by the Ordering Activity during the Term, on the same basis as applies to such mainframe CA Software, even if CA then determines to charge a separate license fee for the mainframe New Product to CA's other licensees.

10.2 Such rights shall not extend to any Hardware provided under this Agreement. Notwithstanding anything to the contrary in the Agreement by and between the parties hereto (i) the Distributed CA Software herein shall not be construed as a "New Product" for the purposes of any prior agreement between the parties; and (ii) the provisions of any "New Product" provision in any prior agreement shall not apply to the distributed CA Software herein or any subsequent license for CA Software.

11. NIMSOFT ON PREMISE

11.1. **The following terms are modified or added for all Nimsoft transactions to the extent consistent with U.S. Federal law:**

11.1.1. **Section 2.4**: "Nimsoft Software" means the computer software programs, made generally available and licensed to a Ordering Activity under this Module, including all Versions, Releases, provided as part of Support if applicable."

11.1.2. **Section 4.1: "**If Support is purchased by Ordering Activity, CA will provide Ordering Activity with technical support for the Nimsoft Software, according to the Support specified in the Authorized CA Partner's order with CA, to operate according to the Documentation, help desk support and Maintenance for the Nimsoft Software pursuant to the following: http://www.nimsoft.com/content/dam/nimsoft/documents/un-secure/agreements/nimsoft-us-support-agreement.pdf."

11.1.3. **Add as Section 15: "15. REPORTS.** Ordering Activity agrees to prepare and submit monthly reports to the CA Authorized Reseller and CA that shall include, without limitation, information detailing the use of the Nimsoft Software pursuant to the license metrics applicable to the Software ("Report"). Ordering Activity shall submit each Report to CA Authorized Reseller and CA on the fifteenth day of each calendar month."

11.1.4. **Add as Section 16:** "**16. OVERAGE**. If the Report shows the Ordering Activity has exceeded the Authorized Use Limitation at any time during a month, such Report shall constitute the basis for a claim to the relevant Contracting Officer pursuant to the Contract Disputes Act and FAR 52.233-1. In no event may the Perpetual License or Subscription License quantity be lowered below the original number ordered."

12. GENERAL TERMS

12.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this

Channel Software Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

Attachment A to Channel Software Module
Definitions and License Metrics

APPLICABILITY

The following definitions and License Metrics shall apply to the CA Software licensed by Ordering Activity to the extent such terms and/or CA Software are included in Ordering Activity's agreement with Authorized CA Partner or Prime Contractor:

Arcot

"Tier Servers" means single server of any tier up to and including Tier 9 Server. "Server" shall designate a specialized computer or a serial of processors assigned to store and to distribute information to and from Customer's personal computer (workstations). Linked to a company network, it enables a shared access to the files and a printing service support. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis.

CA Access Control Premium Edition

"Managed Device" means a virtual or physical machine to which the CA Software controls access.

CA Access Control Privileged User Password Management (PUPM)

"Managed Device" means a virtual or physical system or application whose privileged account passwords are being managed by the CA Software, including but not limited to operating system instances, databases, applications, Command Line Interface Software Development Kits, Open Database Connectivity/Java Database Connectivity applications, Windows services and managed tasks, and managed configuration files. When CA Software is used (i) in connection with a Managed Device or (ii) in connection with a virtual or physical system or application that leverages or interoperates with a Managed Device (a "Password Consumer System or Application"), each such use of the CA Software shall be counted for the purposes of determining the Authorized Use Limitation.

CA Automation Suite for Data Centers

A "Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores. CA Configuration Automation program is included in the delivery of CA Automation Suite for Data Centers for use in server environments managed under CA Automation Suite for Data Centers license. Use of this program with server environments not managed by CA Automation Suite for Data Centers requires a separate license for additional fees. Systems Performance for Infrastructure Manager (SystemEDGE) and Virtual Assurance for Infrastructure Manager AIMS components are included in the delivery of the CA Automation Suite for Data Centers for use only with this product. Use of these components with other CA products requires a separate license for additional fees.CA IT Client Management solution consists of CA Software Delivery, CA Asset Management, CA Remote Control programs and is included in the delivery of the CA Automation Suite for Data Centers. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.CA Asset Intelligence and CA Patch Manager programs are included in the delivery of the CA Automation Suite for Data Centers. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.CA Process Automation program is included in the delivery of CA Automation Suite for Data Centers. CA Process Automation includes two Orchestrators, all non-Premium Connectors, unlimited Agents and 75 Concurrent Processes per Orchestrator. Additional Orchestrators and Premium Connectors are available as an add-on option at additional cost. "Agent" means a single installation of the agent software component of the CA Process Automation program on a specific operating system which can be identified as unique host identification on a physical or virtual hardware server. "Orchestrator" means a single installation of the Orchestrator software component of the CA Process Automation program on a specific operating system which can be identified as unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator. "Connector" is the software program connecting the CA Process Automation program with specific named third party software or other CA software. For example, CA Process Automation Connector For CA Service Desk connects CA Process Automation with CA Service Desk. Each Connector may only be used to connect the CA Software with the specific named third party software or CA software program. "Premium Connector" means a Connector identified by CA in the Order Form. "Process instance" means a single copy of a Process definition that has been scheduled to run (Queued state), is running (Running state), or has completed running (Failed or Completed state) on a particular "Orchestrator".

"Concurrent Processes" means the number of CA Process Automation Process instances that are marked in the Running state within an Orchestrator at any given time.

CA AutoSys Workload Automation

"Instance" means the number of copies of CA AutoSys Workload Automation installed in your physical and/or virtual environment.

CA Clarity Project & Portfolio Manager

"CA Software" means the CA Clarity Project and Portfolio Manager (also known as CA Clarity PPM). CA Clarity PPM is licensed by Environment and the number of Users (Manager, Team Member or Viewer). Customer is granted the right to install and use CA Clarity PPM in not more than three (3) Environments, of which only one (1) may be a production Environment. An "Environment" can consist of any or all of the following, provided that all of the servers in the Environment function as one logical Environment: one or more application servers, search servers, report servers, background servers, and/or database servers. Typical examples of Environments include production Environments, development Environments and test Environments. A production Environment is a computer system used to process an organization's daily work on a real-time operation, not systems used only for development and testing. "Manager User" means Customer's designated users who have full use of and access to the functions within CA Clarity PPM. "Team Member User" means Customer's designated users who have limited rights to the functions within CA Clarity PPM, and may only (i) view data and run reports in all licensed products; (ii) collaboratively participate in processes, discussions and document sharing and receive notifications in all licensed products; (iii) view project tasks and calendars, and report and approve time and project status; and (iv) enter and view status of ideas. "View Only User" means Customer's designated users who have limited rights to the functions within CA Clarity PPM and may only (i) view data and run reports; (ii) originate idea workflows, and participate in the continuation of those workflows.

CA Client Automation

A "Managed System" is any physical or virtual computer system that can host an operating system, including, but not limited to, a desktop computer or laptop computer, used by an end-user as part of their job function to access data, applications and resources, that is administered or managed by CA Client Automation by way of a management infrastructure, whether a CA management agent resides on the system or not. This includes laptops, desktops and virtual desktops running Windows, Macintosh and Linux operating systems, and it excludes Windows Servers, Linux Servers and UNIX systems. The management infrastructure components, such as Domain Manager, Scalability Server, and System Engine, that run on server platforms do not require a separate license, except if these systems themselves are being managed by an active agent for purposes other than serving as the CA Client Automation management infrastructure.

CA Client Automation consists of:
CA IT Client Manager
CA Patch Manager
CA Desktop Migration Manager
CA Asset Intelligence
CA Workflow for CA IT Client Manager (it is included in the delivery of CA Client Automation for use only for automating workflows inside CA Client Automation and between CA Client Automation and other software programs)

CA Configuration Automation:

The CA Software is licensed by the number of Physical Sockets. A "Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Database Performance

CA Database Performance is licensed by the number of CPUs when used as a distributed product. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously. With the Authorized Use Limitation as "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with databases monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with databases monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing databases(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

CA Systems Performance for Infrastructure Managers (formerly known as "CA SystemEdge") is a separate program included in the delivery of CA Database Performance. Customers can use this program only for communication with other CA Technologies tools and/or monitoring CA Technologies software systems only. Full functionality of the program to monitor and manage servers requires a separate license with additional fees.

CA DLP

CA DLP includes CA DLP Enterprise Suite, CA DLP Platform & Surveillance, CA DLP Endpoint, CA DLP Stored Data, CA DLP Message Server and CA DLP Network. CA DLP Network and CA DLP Enterprise Suite (which includes CA DLP Network) require and may only be used on a licensed CA DLP Network Appliance.

"CA DLP Network Appliance" means the hardware that operates the CA DLP Network. "User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless specified on the Order Form, a User shall not be counted more than once or a concurrent basis. If an Appliance is included with the CA Software, Support for an Appliance is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Enterprise Log Manager

"Agent" means a single installation of the agent software on a specific operating system instance which can be identified as a unique host identification on a hardware server. A hardware server may have multiple operating system instances installed on it (through partitioning or virtualization). Each instance of the operating system on a partitioned/virtualized server must license an agent if required for job scheduling purposes. "Node" means, in a communications system, a network junction or connection point. Any system or device connected to a network is also called a node or cluster. "Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA ESP Workload Automation
(MIPS Based license. Operating System is IBM z/OS)

CA ESP Workload Automation is licensed by the specified number of MIPS (the "Authorized Use Limitation in MIPS"). "MIPS" means millions of instructions per second. The MIPS capacity of a computer shall be calculated by reference to CA's published schedules of the MIPS capacity and if a computer isn't listed then the manufacturer's published specifications should apply. In the event that any particular computer is not accounted for on CA's schedule, the manufacturer's published specification of MIPS capacity shall control. Further, in the event a special purpose processor, designed to perform one or more dedicated functions, is being used as a general purpose processor, CA shall treat such processor as a general purpose processor for purposes of calculating Authorized Use Limitation in MIPS. "Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated. Customer may use the CA Software only on the specific computers upon which the CA Software is installed to run at the Customer Site or on computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software, subject to the aggregate MIPS capacity not exceeding the Authorized Use Limitation in MIPS.

CA Fast Unload for Distributed Databases:

The CA Software is licensed by the number of servers. “Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Federation Manager:

(a) “Federate” means to link or bind two or more entities together, enabling identity, account, attribute, authentication, and authorization federation across different trust realms.
(b) “Federation” means a relationship or an association between a specific system entity’s identified users, partners or accounts.
(c) “Federation Partner” means an internal or external entity (i) for which a unique federation configuration is required in order to join a Federation, and (ii) with whom Customer interoperates using Federation Manager, with or without SAML AA.
(d) “Federation Partnership Licensee” means the Federation Partner designated by Customer as licensed to use SAML AA or Federation Manager in accordance with the provisions of the Agreement and who has agreed in writing to Customer terms and conditions substantially similar to the Federation Manager and SAML AA license provisions contained herein, as well as the confidentiality provisions contained in the Agreement. Such Federation Partnership Licensee shall not have any right to further copy, distribute, or otherwise transfer such software or any rights therein, notwithstanding any provision of the Agreement to the contrary. With regard solely to such Federation Partner’s use of the Licensed Programs in accordance herewith, the term “Customer” in the Agreement includes such Federation Partner.
(e) “Federation User” means any user who is allowed to use a Federation via the specific configuration of Federation Manager that Customer deploys. A Federation User shall not be counted more than once or on a concurrent basis.

CA GEN ENC Cross-Gen Opt Linux

“Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. “Non Tier Servers” means single server of any tier up to and including Tier 9 Server.

CA GEN Implementation Toolset

“Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. “Non Tier Servers” means single server of any tier up to and including Tier 9 Server.

CA GEN TRANSACTION Enabler

“Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. “Non Tier Servers” means single server of any tier up to and including Tier 9 Server.

CA GEN TRANSACTION Enabler User Fnl

“Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. “Non Tier Servers” means single server of any tier up to and including Tier 9 Server.

CA GEN WRKSTN Cross-Gen Linux

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA Identity Manager

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA Identity Manager. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Internal User" is an intranet User defined as an employee or contractor of the Customer. CA Identity Manager may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor with any users of CA Identity Manager separately licensed by such contractor. "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA Identity Manager separately licensed by such vendor or partner.

CA Infrastructure Insight

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Insight consists of CA Spectrum Infrastructure Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Insight for use only for monitoring the databases included in CA Infrastructure Insight. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Insight for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Insight. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additional fees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Infrastructure Management

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Management consists of CA Spectrum Infrastructure Manager, CA eHealth Performance Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Management for use only for monitoring the databases included in CA Infrastructure Management. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Management for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Management. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additional fees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Infrastructure Performance

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Performance consists of CA eHealth Performance Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Performance for use only for monitoring the databases included in CA Infrastructure Performance. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Performance for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Performance. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additional fees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Insight Database Performance Manager

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.CA Systems Performance for Infrastructure Managers (formerly known as "CA System Edge") Limited Use, is a separate program included in the delivery of CA Insight Database Performance Manager. The customers can use this program only for communication with other CA Technologies tools and/or monitoring CA Technologies Software systems only. Full functionality of the program to monitor and manage servers requires a separate license with additional fees.

CA IT Asset Manager

"CA Software" means the CA IT Asset Manager and CA Software Compliance Manager. A "Managed System" is any physical or virtual desktop, laptop, server, and tablet computer that may be tracked and/or managed by the CA Software, based upon user-supplied unique designations to identify such computers, regardless of use purpose including non-production, spares, or disaster recovery. If the optional component CA Software Compliance Content Subscription is listed on the applicable Order Form, Customer is granted a term license to use such content with CA Software Compliance Manager or CA IT Asset Manager beginning on the Term Start Date and ending on the Term End Date. The subscription fees for CA Software Compliance Content Subscription include the right to receive content updates during the Term of the content subscription. Such license for CA Software Compliance Content Subscription shall renew at the option of the Ordering Activity and be extended for successive periods equivalent to the original subscription Term, subject to the parties' agreement concerning fees to be paid during each such extended term. Use of the CA Software is limited as to several components included unless separately licensed. Software technology for Software Distribution, Remote Control and Asset Discovery and Inventory (CA IT Client Management) are included with CA Software Compliance Manager and CA IT Asset Manager, however the only authorized use is the ability to import Microsoft SMS 2003 or Microsoft SystemCenter Configuration Manager 2007 through the CA Asset Converter for Microsoft SMS, importing inventory from other third party discovery tools using the Asset Collector technology and CA IT Client Manager technology. Explicitly, Customer is not licensed to use the software distribution, remote control technologies as well as the full asset inventory and discovery agents. Use of the CA Software or CA Software Compliance Content Subscription is not a substitute for Customer's compliance with any laws (including but not limited to any act, statute, regulation, requirement, rule, standard, directive, administrative order, executive order, etc. (collectively, "Laws")). Customer should consult with competent legal counsel regarding any such Laws. Use of the CA Software or CA Software Compliance Content Subscription is not a substitute for Customer's compliance with its contractual obligations. The CA Software and CA Software Compliance Content Subscription require Customer to (i) manually or electronically enter or (ii) make decisions regarding software license data and other information for purposes of tracking authorized use, compliance with its software license contractual obligations and other information ("Data Entry"). Notwithstanding the provisions of any warranty to the contrary, CA makes no warranty with respect to the CA Software or CA Software Compliance Content Subscription failure, error, omission or inaccuracy to the extent that any such failure, error, omission or inaccuracy relates, in whole or in part, to Data Entry errors, omissions, decisions, inaccuracies, misinterpretations or otherwise.

CA IT Client Manager

"Managed System" is any physical or virtual computer system that can host an operating system, including, but not limited to, a desktop computer, server, or laptop computer, that is administered or managed by the CA Software (IT Client Manager / IT Inventory Manager) by way of a CA management agent, whether it resides on the asset or not. A "Non-CA managed system" has their inventory gathered by a non-CA management agent; however, the information about that asset is still stored in the Management Database (MDB). This asset information may have been obtained using the SMS Connector or Asset Collector. If Customer is licensed for CA IT Client Manager Patch Subscription, Customer is granted a term license to use such program with CA IT Client Manager beginning on the Term Start Date and ending on the End Date for the subscription term. The term license for the CA IT Client Manager Patch Subscription shall renew at the Ordering Activity's option and be extended for successive periods equivalent to the original term, subject to the parties' agreement concerning fees to be paid during each extended term.

CA Mainframe for IBM Rational Developer for System z Unit Test (CA Mainframe Suite for RDz UT):

a) Additional license rights to the CA software program(s) referenced below ("CA Software") are provided under the following terms and conditions in addition to any terms and conditions referenced (i) on the Order Form entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software and (ii) in the software license agreement between you and CA for the CA Software. These terms shall be effective from the effective date of the Order Form.

b) **Program Name:** CA Mainframe Suite for IBM Rational Developer for System z Unit Test ("RDz UT")

c) Specified Operating Environment

The license rights set forth herein apply only to CA Software separately licensed from CA for the z/OS environment and for use hereunder only in the IBM RDz UT environment.

d) CA Software

CA Software for IBM RDz UT Environment:

CA 1™ Tape Management, CA TLMS® Tape Management
CA ACF2™, CA ACF2™ Option for DB2
CA Aion® Business Rules Expert
CA Auditor for z/OS, CA Cleanup
CA Bundl®
CA Cleanup
CA Compliance Manager for z/OS
CA Database Management for DB2 for z/OS
CA Database Management for IMS for z/OS
CA Datacom®
CA Deliver™
CA Disk™ Backup and Restore
CA Dispatch™
CA Easytrieve®
CA Endevor® Software Change Manager
CA FileMaster™ Plus, CA FileMaster™ Plus IMS
CA Gen
CA Gener/OL
CA IDMS™
CA InterTest™ for CICS, CA InterTest™ Batch
CA JCLCheck™ Workload Automation
CA JobTrac™ Job Management
CA Librarian®
CA Mainframe Application Tuner
CA Mainframe Software Manager™
CA NetMaster® File Transfer Management, CA NetMaster® Network Automation, CA NetMaster® Network Management for SNA, CA NetMaster® Network Management for TCP IP
CA Optimizer®/II
CA Panvalet®
CA Roscoe®

CA Scheduler® Job Management
CA Spool™
CA SymDump® Batch, CA SymDump® for CICS
CA Telon®
CA Top Secret®, CA Top Secret® Option for DB2
CA UFO™
CA View®
CA Workload Automation CA 7® Edition, CA Workload Automation ESP Edition, CA Workload Automation Restart Option EE, CA Workload Automation Restart Option for z/OS Schedulers
CA XCOM™ Data Transport®

e) Licensing Model and Terms

The license rights set forth herein authorize you to use CA Software for which you are separately licensed only in the IBM RDz UT environment for non-production purposes. During the term of this license, you must also be licensed to use the IBM RDz UT environment. Use of the CA Software in any other environment or in the RDz UT environment for production purposes is expressly prohibited. This restriction does not change your existing license rights to use the CA Software in a production environment. A production environment is a computer system used to process an organization's daily work on a real-time operation and is not a system used only for development and testing. During the term of this license, if you license additional CA Software, the license rights granted herein apply to such subsequently licensed CA Software.

The license rights are provided on a “per Seat” basis. “Seat” means a single person or identity whose access and use rights can be authenticated, authorized, or administered, or who has the ability to view content aggregated or managed by the CA Software. In general, a Seat shall not be counted more than once or on a concurrent (logged-in) basis. One Seat license shall authorize you to use any of the CA Software for which you are separately licensed in the RDz UT environment. The term of this license (the “Term”) is the lesser of: (i) one (1) year; (ii) the term end date for the applicable separately licensed CA Software; or (iii) the term end date for your use of the IBM RDz UT environment. Any termination under clauses (ii) or (iii) immediately above shall not result in refund of any license fees paid hereunder. Subject to the limitations set forth in clauses (i) (ii) and (iii) immediately above, any renewal or extension of the license term for the separately licensed CA Software or the IBM RDz UT environment, as the case may be, shall continue the Term of this agreement for the period identified above. If you have multiple CA Software products with different term end dates, the license rights granted herein terminate as to each specific CA Software product in the lesser of one (1) year or when the applicable term license for such CA Software ends. Termination of license rights hereunder shall not terminate your license to any CA Software product.

CA does not provide support for the CA Software in the RDz UT environment. Any issues with the CA Software in the RDz UT environment must be reproduced by you in the z/OS environment and reported as such through CA Technologies normal support process for the CA Software.

CA NetQoS NetVoyant

"Device” means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines. Endpoint devices used solely as IP telephones are not considered to be Devices, unless the CA Software is specifically licensed by the number of phones. For the purposes of CA NetQoS Unified Communication Monitor only, endpoint devices used solely as IP telephones are considered to be Devices. When the Authorized Use Limitation is “Device”, the calculation with respect to the number of Licenses is determined as follows:

1. For network-connected devices, in non-virtual server environments, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

2. For network-connected devices, in non-virtual server environments, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, in non-virtual environments, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA NetQoS Reporter Analyzer

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines. Endpoint devices used solely as IP telephones are not considered to be Devices, unless the CA Software is specifically licensed by the number of phones. For the purposes of CA NetQoS Unified Communication Monitor only, endpoint devices used solely as IP telephones are considered to be Devices. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

1. For network-connected devices, in non-virtual server environments, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

2. For network-connected devices, in non-virtual server environments, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, in non-virtual environments, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA RegFort:

CA RegFort is licensed by the number of Users or Issuance.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA RegFort or who has the ability to view content aggregated or managed by CA RegFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

"Issuance" means any activity in the life cycle of a Public Key Infrastructure credential that is managed by CA RegFort, including, but not limited to, creation of a new credential, revocation, renewal, re-issue or update of the credential.

"RegFort Client" means a portion of CA RegFort which enables end-users to interface with smartcards and tokens.

Limited License Grant. In addition to the rights granted in the applicable license agreement, CA grants Customer and its affiliates a nonexclusive license to distribute RegFort Client to end-users. Customer may use Customer's logo and name with the RegFort Client. No title to or ownership of the RegFort Client is transferred to Customer.

CA RiskFort:

CA RiskFort is licensed by the number of Users.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA RiskFort or who has the ability to view content aggregated or managed by CA RiskFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

CA Role and Compliance Manager

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. An "Internal User" is an intranet User defined as an employee or contractor of the Customer. CA Role and Compliance Manager may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor with any users of CA Role and Compliance Manager separately licensed by such contractor. An "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA Role and Compliance Manager separately licensed by such vendor or partner.

CA Server Automation

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Systems Performance for Infrastructure Manager (SystemEDGE) and CA Virtual Assurance for Infrastructure Manager AIMS components are included in the delivery of the CA Server Automation for use only with this product. Use of these components with other CA products requires a separate license for additional fees.

CA IT Client Management solution consists of CA Software Delivery, CA Asset Management, CA Remote Control programs and is included in the delivery of the CA Server Automation. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.

CA Asset Intelligence and CA Patch Manager programs are included in the delivery of the CA Server Automation. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.

CA Service Desk Manager

"CA Software" and "SDM" mean the CA Service Desk Manager – Analyst License, CA Service Desk Manager - Full License, or CA CMDB Manager Servers described herein in object code form. CA Service Desk Manager-Full License and CA Service Desk Manager-Analyst License are licensed on a Concurrent Analyst basis. In CA Service Desk Manager-Full License, CA Service Desk Manager-Analyst License, the authorized users are assigned various roles based upon the functions needed to accomplish designated tasks. "Concurrent Analyst", in the context of CA Service Desk Manager, means a software license that is based on the number of simultaneous (concurrent) users accessing the program. For the purpose of SDM, all roles (for example: Analyst, Manager, Administrator), and programmatic API and/or web services calls require a license. The Software does not prohibit additional users from access, but does log a license exception for auditing purposes. Customer is entitled to have the specified number of Concurrent Analysts access CA Service Desk Manager simultaneously. For CA Service Desk Manager-Full License, CA Service Desk Manager-Analyst License, You are also licensed for End-User Self-Service, which is granted to the employee and customer roles to allow for the creation, modification, and closure of a ticket on their own behalf, but not on behalf of someone else. CA Service Desk Manager-Full License includes a limited entitlement to CA Cohesion, and use of CA Cohesion is restricted to a maximum of one hundred (100) Managed Servers. Use for additional Servers requires additional licenses for CA CMDB Managed Server. CA Service Desk Manager-Analyst License does not include the CA Cohesion entitlement. CA CMDB Managed Servers is licensed by the number of Servers. "Managed Servers" means a virtual or physical Server managed by CA Software. "Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Service Desk Manager includes a limited entitlement to CA Business Intelligence. This entitlement is restricted to use within the context of reporting for SDM only. Specifically, SDM reports created using CA Business Intelligence may access and incorporate data created by, derived from, or used by SDM or third party data sources, provided that such data facilitates or augments data for Customer's use of SDM.

CA Service Desk Manager includes a limited entitlement to CA Process Management for Workflows. This entitlement is restricted to use within the context of Workflows associated with SDM only. This entitlement includes: the Service Desk Manager connector; three (3) Custom Operators; and five (5) Agents. This entitlement does not include any Premium Connectors. Multiple Orchestrators can be deployed with the constraints specified herein. There are no license limitations on the number of concurrent processes per Orchestrator.

For the purpose of CA Process Management for Workflows, "Agent" means a single installation of the agent software component of the CA Process Management for Workflows on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server.

For the purpose of CA Process Management for Workflows, "Connector" is the software program connecting CA Process Management for Workflows with specifically named third-party software or other CA software. For example, "CA Process Management for Workflows Connector for CA Service Desk Manager" connects CA Process Management for Workflows with CA Service Desk Manager. Each Connector may only be used to connect the CA Software with the specific named third-party software or CA software program.

For the purpose of CA Process Management for Workflows, "Custom Operator" means a type of automation object within the CA Process Management for Workflows that can be created to enhance, modify, or restrict the capabilities of an existing "Connector".

For the purpose of CA Process Management for Workflows, "Orchestrator" means a single installation of the Orchestrator software component of CA Process Management for Workflows on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator.

CA SiteMinder

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. An "Internal User" is an intranet User defined as an employee or contractor of the Customer. CA SiteMinder may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor with any users of CA SiteMinder separately licensed by such contractor. An "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA SiteMinder separately licensed by such vendor or partner.

CA SOA Security Manager

"Secured Web Service" means a software system designed to support interoperable machine-to-machine interaction over a network which needs to be secured from unauthorized access, software routines or components that is or are intended to disable, erase, or otherwise harm software, equipment, or data, or cause other similar damage. This web service can be a URI or web services End point defined in a WSDL file. "URI" (Uniform Resource Identifier) means a compact string of characters for identifying an abstract or physical resource. “End point” means a specific location for accessing a web service using a specific protocol and data format. "WSDL" (Web Service Definition Language) means an XML (Extensible Markup Language) format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. "User" means a single person, application or identity listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software or who has the ability to view content aggregated or managed by CA SOA Security Manager. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

CA SOA Security Manager with Gateway

CA SOA Security Manager is licensed in number of Secured Web Services and Users. CA SOA Security Gateway is licensed in number of Instances. "Secured Web Service" means a software system designed to support interoperable machine-to-machine interaction over a network which needs to be secured from unauthorized access, software routines or components that is or are intended to disable, erase,

or otherwise harm software, equipment, or data, or cause other similar damage. This web service can be a URI or web services End point defined in a WSDL file. "URI" (Uniform Resource Identifier) means a compact string of characters for identifying an abstract or physical resource. “End point” means a specific location for accessing a web service using a specific protocol and data format. "WSDL" (Web Service Definition Language) means an XML (Extensible Markup Language) format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. "User" means a single person, application or identity listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA SOA Security Manager or who has the ability to view content aggregated or managed by CA SOA Security Manager. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis. "Installation" means the number of copies of CA SOA Security Manager installed in the Customer’s physical and/or virtual environment.

CA Spectrum Infrastructure Manager

"Managed Network Device” means a virtual or physical network-connected device with less than 200 ports that is managed by CA Spectrum Infrastructure Manager and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, virtual or physical servers, and virtual or physical machines, but excluding endpoint devices such as IP telephones.

CA Spectrum Service Assurance

“Site” or “Installation” means use of CA Spectrum Service Assurance in a data center comprised of one or more CPUs conforming to the following conditions: Two or more CPUs will be considered part of the same site if (i) the CPUs are located in a single building, (ii) each CPU shares access to data storage and peripheral devices with one or more of the other CPUs without requiring any programming interface to another CPU, and (iii) the CPUs function as a data processing facility under common data processing operations supervision. Use of CA Spectrum Service Assurance on two or more CPUs will be considered multiple and separate sites if all of the foregoing conditions of a single site are not satisfied, regardless of (i) whether they occupy different floors or locations in the same building or share the same mailing location address, or (ii) the extent to which the CPUs are integrated within a network or serve a functional role as part of a larger data processing organization. Customer is granted the right to deploy CA Spectrum Service Assurance at the Sites with the addresses listed in the Order Form. Customer may change and amend the addresses of the Sites by notice to CA providing that the total number of Sites listed does not exceed the number listed in the Order Form. “Connection” means a data source indicated by CA Spectrum Service Assurance to have a connector status of “Online”. A Connection may consist of a connection to a CA Software product (i.e. CA Wily, CA Spectrum), a third party product (i.e. HPOV), or a custom application. “Data source” means any software application that provides data to CA Spectrum Service Assurance.

CA SYSVIEW for CA Wily APM

Customer is granted a limited license to use CA SYSVIEW for CA Wily APM solely for the integration with CA Wily APM or CA Wily Introscope 8.2 or above (“CA Wily”). With this license, Customer is only authorized to install, configure and use CA SYSVIEW for CA Wily APM components to support its authorized use with CA Wily to provide mainframe performance metrics to CA Wily and trace transactions tagged by CA Wily that perform activity on the mainframe. Customer may not use CA SYSVIEW for CA Wily APM for other purposes. Any additional use requires a separate non-restricted license. In the event Customer chooses to increase its Authorized Use for CA Wily, Customer must also increase its Authorized Use for CA SYSVIEW for CA Wily APM and pay all applicable additional license and maintenance fees related thereto in order to use CA SYSVIEW for CA Wily APM with such increased CA Wily capacity. Additional use of CA Wily without obtaining a separate non-restricted license may be the basis for filing a claim with the relevant Contracting Officer under the Contract Disputes Act and FAR 52.233-1.

CA TSreorg for Distributed Databases

“Server” means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Virtual Assurance

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

If an Appliance is included with the CA Software, Support for an Appliance is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Virtual Automation

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Virtual Configuration

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Virtual Performance Management (CA VPM)

"CPU" or "Processor" means central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A Processor may not exceed a maximum of 12 processing cores.

CA WebFort:

CA WebFort is licensed by the number of User Credentials and Users.

"Credential" means an attestation of qualification, competence, or authority issued to a User by the CA Software.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA WebFort or who has the ability to view content aggregated or managed by CA WebFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

"User Credentials" means the number of Credentials set forth on the Order Form to be issued to the Users who are authorized to access and use CA WebFort. Each User may have more than one credential for different verification methods.

"ArcotID Client" or "ArcotOTP Client" means portions of CA WebFort which enable end-users to use the ArcotID and ArcotOTP credentials.

Limited License Grant. In addition to the rights granted in the applicable license agreement, CA grants Customer and its affiliates a nonexclusive license to distribute the ArcotID Client or ArcotOTP Client to end users. Customer may use Customer's logo and name with the ArcotID Client or ArcotOTP Client. No title to or ownership of the ArcotID Client or ArcotOTP Client is transferred to Customer.

CA Wily Application Performance Management v9 (CA Wily APMv9)

CA Wily APMv9 is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously ("Virtual Machine Technology"). When the

Authorized Use Limitation is “CPU” or “Processor”, the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is “MSUs”, “zAAPs”, or “zIIPs” (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An “LPAR” means the division of a computer’s processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is “IFLs”, the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

CA Wily Transaction Impact Monitor (“TIM”) “Software Appliance” means the software running TIM on Customer’s network feed to capture http/https transactions necessary for the Customer Experience analysis portion of CA Wily APMv9. Customer is responsible for providing hardware on which to run the TIM Software Appliance that meets CA’s specifications. Customer must license a copy of the TIM Software Appliance for each physical server (regardless of the number of CPUs) on which a TIM Software Appliance will be installed and configured.

CA Wily Application Performance Management (CA Wily APM)

CA Wily APM is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units (“MSUs”) and number of System z Application Assist Processors (“zAAPs”) and number of System z Integrated Information Processors (“zIIPs”) or (b) number of integrated facilities for Linux (“IFLs”), when used in the mainframe environment. “CPU” means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously. When the Authorized Use Limitation is “CPU” or “Processor”, the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is “MSUs”, “zAAPs”, or “zIIPs” (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An “LPAR” means the division of a computer’s processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is “IFLs”, the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by CA Wily APM.

An Appliance is a CA-supplied physical server (“Hardware”) that is bundled with and used to operate the CA Software licensed by Customer which is pre-installed on the Hardware. Support is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com. Customer must acquire at least one license (per CPU, MSU or IFL) in order to purchase a CA Wily Transaction Impact Monitor (“TIM”) or CA Wily Transaction Event & Statistics Server (“TESS”). Both a TIM and a TESS are required for any production installation. CA Wily Solutions for Lab Environments (“Wily LAB”) is a single Appliance that contains TIM and TESS capabilities but is not supported for a production environment. The Wily LAB system includes one CPU license for CA Wily APM at no additional charge.

CA Wily Customer Experience Manager (CA Wily CEM)

CA Wily CEM is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units (“MSUs”) and number of System z Application Assist Processors (“zAAPs”) and number of System z Integrated Information Processors (“zIIPs”) or (b) number of integrated facilities for Linux (“IFLs”), when used in the mainframe environment. “CPU” means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously (“Virtual Machine Technology”). When the Authorized Use Limitation is “CPU” or “Processor”, the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is “MSUs”, “zAAPs”, or “zIIPs” (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An “LPAR” means the division of a computer’s processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is “IFLs”, the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

An Appliance is a CA-supplied physical server (“Hardware”) that is bundled with and used to operate the CA Software licensed by Customer which is pre-installed on the Hardware. Support is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com. Customer must acquire at least one license (per CPU, MSU or IFL) in order to purchase a CA Wily Transaction Impact Monitor (“TIM”) or CA Wily Transaction Event & Statistics Server (“TESS”). Both a TIM and a TESS are required for any production installation. CA Wily Solutions for Lab Environments (“Wily LAB”) is a single appliance that contains TIM and TESS capabilities but is not supported for a production environment. The Wily LAB system includes one CPU license for CA Wily CEM at no additional charge.

CA Wily Introscope

CA Wily Introscope is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously ("Virtual Machine Technology"). When the Authorized Use Limitation is "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is "MSUs", "zAAPs", or "zIIPs" (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An "LPAR" means the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications. When the Authorized Use Limitation is "IFLs", the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

CA Workload Automation

"Instance" means the number of copies of the CA Software installed in the Customer physical and/or virtual environment.

CA XCOM Data Transport for Windows Family Server

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA eHealth Performance Manager

"Managed Network Device" means a virtual or physical network-connected device with less than 200 ports that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, virtual or physical servers, and virtual or physical machines, but excluding endpoint devices such as IP telephones.

Mainframe CPU CA Software only

The CA Software is licensed by the specified number and model of CPU (the "Authorized Use Limitation"). "CPU" shall mean the central processing unit(s) capable of running the CA Software. Customer may only use CPUs specified when licensing the licenses herein and upon which the CA Software is installed and runs ("Designated CPUs"). Customer may change the Designated CPU on providing written notice to CA provided that such replacement CPU is of the same or lower CPU tier/power rating to the Designated CPU (save that Customer may

require an authorization key from CA in order to commence use of such CPU). Should Customer wish to add to the number of Designated CPUs or upgrade the then current Designated CPU(s) to a CPU with greater tier/power rating, Customer may elect to do so by providing CA with prior written notice of such additional CPU and/or upgrade to the Designated CPU(s) and by executing an order form to effect such addition/change and purchasing the applicable license.

Mainframe MIPS CA Software only

The CA Software is licensed by the specified number of MIPS (the "Authorized Use Limitation in MIPS"). "MIPS" means millions of instructions per second. The MIPS capacity of a computer shall be calculated by reference to CA's published schedules of the MIPS capacity and if a computer isn't listed then the manufacturer's published specifications should apply. Further, in the event a special purpose processor, designed to perform one or more dedicated functions, is being used as a general purpose processor, CA shall treat such processor as a general purpose processor for purposes of calculating Authorized Use Limitation in MIPS. "Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated. Customer may use the CA Software only on the specific computers upon which the CA Software is installed to run at the Customer Site or on computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software, subject to the aggregate MIPS capacity not exceeding the Authorized Use Limitation in MIPS.

Mainframe MSU CA Software only

The CA Software is licensed by the specified number of MSU (the "Authorized Use Limitation in MSU"). "MSU" means millions of service units. The MSU capacity shall be calculated with the aggregate computing power (expressed in millions of service units) by reference to CA's published schedules of the MSU capacity and if a computer isn't listed then the manufacturer's published specifications shall apply of all computers upon which the CA Software is installed to run at the Customer Site ("Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated) or computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software. Customer may use the CA Software subject to the aggregate MSU Capacity not exceeding the Authorized Use Limitation in MSU.

Pervasive Software:

The Pervasive Software is licensed by either by the number of Server or Users. Pervasive Software may be used to build integrations that connect to any authorized CA Clarity environment.

Pervasive Data Integrator Engine/Agent **for CA** Clarity PPM* is licensed by the number of Servers.
* includes one User license of Pervasive Data Integrator Analyst **Studio for C**A Clarity PPM

Pervasive Data Integrator Analyst **Studio for C**A Clarity PPM is licensed by the number of Users**.**

Pervasive Data Profiler Engine for CA Clarity PPM is licensed by the number of Servers.

Pervasive Data Profiler Analyst Studio for CA Clarity PPM is licensed by the number of Users**.**

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the Pervasive Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis.

CA Process Automation:

CA Software means the CA Process Automation software described herein in object code form only.

“Agent” means a single installation of the agent software component of the CA Software on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server.

“Orchestrator” means a single installation of the Orchestrator software component of the CA Software on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator.

"Connector" is the software program connecting the CA Software with specific named third party software or other CA software. For example, CA Process Automation Connector For CA Service Desk connects CA Process Automation with CA Service Desk. Each Connector may only be used to connect the CA Software with the specific named third party software or CA software program.

“Premium Connector” means a Connector identified as “Premium” by CA.

“Custom Operator” means a type of automation object within the CA Process Automation Orchestrator that can be created to enhance, modify, or restrict the capabilities of an existing “Connector”.

“Process” means a type of automation object within CA Process Automation Orchestrator that contains connectors and other logical constructs that define a set of actions that will take place when the “Process” is executed by the Orchestrator.

“Process instance” means a single copy of a Process definition that has been scheduled to run (Queued state), is running (Running state), or has completed running (Failed or Completed state) on a particular “Orchestrator”.

“Concurrent Processes” means the number of CA Process Automation Process instances that are marked in the Running state within an Orchestrator at any given time.

“Power Pack” means a combination of Process definitions, Premium Connectors, Custom Operators and other automation objects that are packaged together to implement a specific solution.

The CA Software is licensed in different editions, as set forth in this Order Form, which authorizes the use of the specified number of Orchestrators, Agents, Connectors, and Concurrent processes (the "Authorized Use Limitation"). The various editions are:

CA Process Automation Player License includes: one Orchestrator, forty Agents, all non-Premium Connectors, and two hundred Concurrent Processes per Orchestrator. This license requires the purchase of either a “Power Pack” or a Services contract for the implementation of a solution that will be executed by the Player. No new automation objects may be created with the Player License. Only modifications of the purchased Power Packs and any Services delivered content is allowed.

CA Process Automation Express License includes: two Orchestrators, forty Agents, all non-Premium Connectors, and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Standard License includes: two Orchestrators, unlimited Agents, three Premium Connectors, all non-Premium Connectors, and two hundred Concurrent Processes per Orchestrator.

CA Process Automation Enterprise License includes: unlimited Orchestrators, unlimited Agents, twenty Premium Connectors, all non-Premium Connectors, and four hundred and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Level 1 Orchestrator includes: one Orchestrator and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Level 2 Orchestrator includes: two Orchestrators and two hundred Concurrent Processes per Orchestrator.

CA Process Automation Level 3 Orchestrator includes: three Orchestrators and four hundred and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Premium Connector License includes the right to use a Premium Connector to connect to a single instance of the target application or system.

CA Process Management for Workflows License includes: unlimited Orchestrators, five Agents, and three Custom Operators. No Premium connectors are available for purchase with this license. The only CA product connectors that are available are those associated with the product(s) providing the entitlement. This is a limited use entitlement and its use is restricted to the context of Workflows associated with the CA product(s) providing the entitlement. The component limits are not cumulative across multiple instances of the license at any individual customer.

The number of concurrent processes executing on any licensed Orchestrator may be exceeded as long as the total number of concurrent processes executing on all licensed Orchestrators is not exceeded. For example, if the license is for two Orchestrators with seventy-five Concurrent Processes per Orchestrator, one hundred Concurrent Processes could be utilized on one Orchestrator so long as only fifty Concurrent Processes are utilized on the second Orchestrator.

Server:

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Virtual Assurance for Infrastructure Managers and CA System Performance for Infrastructure Managers

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

DOCUSIGN, INC.
CORPORATE SUBSCRIBER TERMS AND CONDITIONS
v121008

These Terms and Conditions are incorporated by this reference into the Order Form (collectively referred to as the "Agreement") entered into by DocuSign, Inc. ("DocuSign") and the customer identified in the Order Form ("Subscriber").

1. DEFINITIONS

"Account" means a unique account established by Subscriber to enable its Authorized Users to access and use the Subscription Service and, where applicable, other DocuSign Products.

"Authorized User" means any employee of Subscriber, identified by a unique email address and user name, who is registered under the Account; provided that no two persons may register or use the Subscription Service as the same Authorized User.

"Consulting Services" means any additional professional services to be delivered by DocuSign, such as integration consulting or assistance, custom development, training, and transition services, that are set forth in an Order Form or Work Order as described in Section 15.

"DocuSign API" means the application programming interface that supports interoperation of applications with the Subscription Service.

"DocuSign Products" means the products and services identified on an Order Form, which may include the Subscription Service, the Repository Services, the Consulting Services and any other DocuSign offerings.

"eContract" refers to a contract, notice, disclosure, or other record or document deposited into the System by Subscriber for Processing using the Subscription Service.

"Envelope" means an electronic record containing one or more eContracts consisting of a single page or a group of pages of data uploaded to the System.

"Order Form" means a standard DocuSign order form or any other document separately and specifically approved by DocuSign that describes the DocuSign Products to be purchased by Subscriber and is signed by both parties.

"Personal Data" means any of the following: (a) nonpublic personally identifiable information, including driver's license numbers, national identification numbers such as social security account numbers, credit card numbers, digital identity certificates; (b) personally identifiable financial information regarding a consumer (i) provided by a consumer to a financial institution, (ii) resulting from any transaction with the consumer or any service performed for the consumer by a financial institution, or (iii) otherwise obtained by the financial institution, including any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information; (c) personally identifiable medical or health-related information.

"Process" means any operation or set of operations performed upon Subscriber's data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, accessing, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Repository Services" means the Contract Repository or eVaulting Services, each as defined in the Terms and Conditions for Repository Services (available at http://www.docusign.com/company/terms-and-conditions/eoriginal/v121005), that are made the subject of an Order Form.

"Specifications" means the technical specifications set forth in the "Subscription Service Specifications" available at http://docusign.com/company/specifications.

"Subscription Service" means DocuSign's on-demand electronic signature service, which provides online display, certified delivery, acknowledgement, electronic signature, and storage services for eContracts via the Internet.

"System" refers to the software systems and programs, communication and network facilities, and hardware and equipment used by DocuSign or its agents to provide the Subscription Service.

"Term" means the period of effectiveness of this Agreement, as described in more detail in Section 9 below.

"Transaction Data" means the metadata associated with an Envelope and maintained by DocuSign for the purpose of establishing a digital audit trail, such as transaction history, image hash value, method and time of Envelope deletion, sender and recipient names, email addresses and signature IDs.

2. THE SUBSCRIPTION SERVICE

2.1 During the Term and subject to these Terms and Conditions, DocuSign will provide the Subscription Service in accordance with the Specifications, and Subscriber will have the right to obtain an Account and register its Authorized Users, who may access and use the Subscription Service. The right to use the Subscription Service is: (a) limited to its Authorized Users (accordingly, Subscriber may not resell or otherwise provide or assist with the provision of the Subscription Service to any third party); and (b) conditioned on Subscriber's acknowledgement and agreement with the following:

i) Nothing in this Agreement will be construed to make DocuSign a party to any eContract, and DocuSign makes no representation or warranty regarding the transactions sought to be effected by any eContract;

ii) DocuSign maintains no control of or access to the contents of any eContract, and so the content, quality, and format of any eContract is at all times in the exclusive control and responsibility of Subscriber;

iii) If Subscriber elects to use optional features designed to verify the identity of the intended recipient of an eContract ("Authentication Measures"), DocuSign will apply only those Authentication Measures (if any) selected by the Subscriber, but makes no representations or warranties about the appropriateness of any Authentication Measure and further, assumes no liability for the inability or failure by the intended recipient or other party to satisfy the Authentication Measure or to circumvent it;

iv) Certain types of agreements and documents are excepted from electronic signature laws, such that they cannot be legally formed by electronic signatures, and additionally, various agencies may have promulgated specific regulations that apply to electronic signatures and electronic records. DocuSign assumes no responsibility to determine whether any particular eContract is an exception to applicable electronic signature laws, or whether it is subject to any particular agency promulgations, or whether it can be legally formed by electronic signatures;

v) Subscriber is solely responsible for making available to third parties (including all parties to its eContracts) all contracts, documents, and other records required by applicable law, including, without limitation, electronic signature laws and other laws that may require records relating to a transaction to be retained or made accessible for a certain period of time;

vi) Certain laws or regulations impose special requirements with respect to electronic transactions involving one or more "consumers," such as (among others) requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. DocuSign assumes no responsibility to: (A) determine whether any particular transaction involves a consumer; (B) furnish or obtain any such consents or to determine if any such consents have been withdrawn; (C) provide any information or disclosures in connection with any attempt to obtain any such consents; (D) provide legal review of, or to update or correct any information or disclosures currently or previously given; (E) provide any such copies or access except as expressly provided in the Specifications for all transactions, consumer or otherwise; or (F) otherwise to comply with any such special requirements; and

vii) Subscriber expressly undertakes to determine whether any consumer is involved in any eContract presented by its Authorized Users for Processing, and, if so, to comply with all requirements imposed by law on such eContracts or their formation.

3. SUBSCRIPTION PLANS AND USAGE PRICING

3.1 The pricing, features and options of the DocuSign Products selected by Subscriber are set forth in the Order Form. The Subscription Service is sold on a subscription basis and may be limited by usage ("Envelope Allowance"), or by the number of Authorized Users ("Seats"), or both. Optional features, such as Authentication Measures or fax-back services, may be purchased on a periodic or per-use basis.

3.2 If Subscriber selects an Envelope Allowance Subscription, then Subscriber is allowed to send the number of Envelopes in the Envelope Allowance specified in the Order Form during the Term. All Envelopes sent in excess of the Envelope Allowance will incur a per-Envelope charge that will be invoiced within 30 days of the date first incurred. The total number of Envelopes used is based on the sum of all Envelopes that have been sent for signature or for certified delivery from the Account. An Envelope will be deemed consumed at the time it is sent by an Authorized User, whether or not it has been received by the recipients or the recipients have performed any actions upon any eContract in the Envelope.

3.3 If Subscriber selects a Seat Subscription, then Subscriber is allowed to manually send Envelopes from the number of Seats specified in the Order Form during the Term. A Seat is defined as a natural person manually preparing and sending Envelopes, and excludes the Processing of Envelopes using automated batch or bulk sending operations, or the use of the

DocuSign API for sending Envelopes. If the number of Envelopes sent from a particular Seat or a group of Seats is abusive and/or unduly burdensome (indicating automated Processing), DocuSign will promptly notify Subscriber and the parties will review the use-case scenario as well as any continued monitoring and additional Seats that may be required to be purchased. The number of Seats is determined by the total number of active Authorized Users listed in the membership of an Account at any one time. No two individuals may log onto or use the Subscription Service as the same Authorized User, but Subscriber may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time is equal to or less than the number of Seats purchased. The addition by Subscriber of more Authorized Users than the number of Seats purchased in an Order Form will result in an additional charge for one Seat per additional Authorized User for the remainder of the Term, to be invoiced immediately.

4. ADDITIONAL SUBSCRIBER RESPONSIBILITIES

4.1 Subscriber agrees that it will not use or permit the use of the Subscription Service to send unsolicited mass mailings outside its organization, it being understood that the term "unsolicited mass mailings" includes all statutory and other common definitions, including all Commercial Electronic Marketing Messages as defined in the U.S. CAN SPAM Act.

4.2 Subscriber agrees that it is solely responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, written or audible communications of any nature submitted by any Authorized User or otherwise Processed through its Account.

4.3 Subscriber further agrees not to use or permit the use of the Subscription Service: (a) to communicate any message or material that is defamatory, harassing, libelous, threatening, or obscene; (b) in a way that violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability (other than contractual liability of the parties under eContracts Processed through the Subscription Service); (c) in any manner that is likely to damage, disable, overburden, or impair the System or the Subscription Service or interfere in any way with the use or enjoyment of the Subscription Service by others; or (d) in any way that constitutes or encourages conduct that could constitute a criminal offense.

4.4 Although DocuSign does not monitor the content Processed through the Subscription Service, DocuSign may at any time suspend any use of the Subscription Service and/or remove or disable any content as to which DocuSign reasonably and in good faith believes is in violation of this Agreement. DocuSign agrees to provide Subscriber with notice of any such suspension or disablement before its implementation unless such suspension or disablement is necessary to comply with legal process or prevent imminent harm to DocuSign's System, the Subscription Service or any third party, in which case DocuSign will notify Subscriber of such suspension or disablement as soon as reasonably practicable thereafter.

5. INTELLECTUAL PROPERTY AND TRADEMARK LICENSE

5.1 DocuSign is the owner of various intellectual property and technology rights associated with the Subscription Service, its document management, digital signature, and notary system, including patent, copyright, trade secret, and trademark and service mark rights. Except for the rights expressly granted in this Agreement, DocuSign does not license or transfer to Subscriber or any Authorized User or other third party any of DocuSign's technology or other intellectual property or technology rights. All right, title, and interest in and to DocuSign's technology and intellectual property will remain solely with DocuSign. Subscriber agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or other trade secrets from or about any of the DocuSign Products or DocuSign's technology. DocuSign agrees that data and information provided by Subscriber under this Agreement shall remain, as between Subscriber and DocuSign, owned by Subscriber.

5.2 DocuSign hereby grants to users and licensees of its products and services a limited, revocable, nonexclusive and nontransferable right to use DocuSign's regular trade names, trademarks, titles and logos ("Licensed Marks") solely for purposes of identifying DocuSign's products and services. Details of this trademark license are available at: http://www.docusign.com/trademark-license.

6. CUSTOMER SUPPORT

DocuSign will provide customer support to Subscriber in accordance with the package that is identified on the Order Form, as further detailed at http://www.docusign.com/products/support-plans.

7. eCONTRACT STORAGE AND DELETION

7.1 DocuSign will store in accordance with the Specifications all completed eContracts sent by Subscriber until the termination or expiration of the Agreement, unless otherwise directed by Subscriber. Copies of stored eContracts may be retrieved by Subscriber at any time during that period, provided that following the expiration or termination of the Agreement, Subscriber may

request DocuSign's assistance in retrieving completed eContracts still remaining on the System pursuant to the transition services terms described in Section 9.4.

7.2 Prior to the expiration or termination of this Agreement, Subscriber may elect to purchase post-expiration or post-termination storage services for their completed eContracts. Where Subscriber opts not to purchase storage services, all copies of eContracts may be deleted by DocuSign without prior notice after the period available for transition services has expired pursuant to the terms described in Section 9.4. Subscriber may, at its option and wholly at Subscriber's risk, direct that any eContract be deleted at a time stated by Subscriber and prior to the end of the Term.

7.3 DocuSign may at its sole discretion delete an uncompleted eContract from the System immediately and without notice upon earlier of: a) expiration of the Envelope (where Subscriber has established an expiration for such Envelope, not to exceed 365 days); or b) expiration of the Term.

7.4 DocuSign will retain the Transaction Data permanently, provided that any Transaction Data that constitutes Confidential Information of Subscriber will at all times maintain that status and DocuSign will comply with its obligations in Section 13.

8. FEES AND PAYMENT TERMS

8.1 Subscriber will pay DocuSign the amounts set forth in each Order Form. An Order Form is not binding until it is executed by both DocuSign and Subscriber, at which point it will be deemed to be incorporated into this Agreement. Unless otherwise specified in an applicable Order Form, the first invoice will be submitted to Subscriber within 30 days after the Order Start Date, and Subscriber will pay all amounts due within 30 days of the date of the applicable invoice.

8.2 If Subscriber's usage under an Envelope Allowance Subscription exceeds the Envelope Allowance prior to the end of the Term, the unpaid balance of the Order Form for such Envelope Allowance Subscription shall become immediately due and payable.

8.3 Any undisputed amount not paid when due will be subject to finance charges equal to 1.5% of the unpaid balance per month or the highest rate permitted by applicable usury law, whichever is less, determined and compounded daily from the date due until the date paid. Subscriber will reimburse any costs or expenses (including reasonable attorneys' fees) incurred by DocuSign to collect any undisputed amount that is not paid when due. DocuSign may accept any check or payment in any amount without prejudice to DocuSign's right to recover the balance of the amount due or to pursue any other right or remedy. Amounts due to DocuSign under this Agreement may not be withheld or offset by Subscriber for any reason against amounts due or asserted to be due to Subscriber from DocuSign. All amounts payable under this Agreement are denominated in United States dollars, and Subscriber will pay all such amounts in United States dollars.

8.4 Taxes. Other than federal and state net income taxes imposed on DocuSign by the United States, Subscriber will bear all taxes, duties, and other governmental charges (collectively, "taxes") resulting from this Agreement or transactions conducted in relation to this Agreement or the DocuSign Products. If a tax is imposed on DocuSign by a jurisdiction outside the United States, Subscriber will not be obligated to bear that tax to the extent: (a) the tax is allowable as a credit against the United States federal income taxes of DocuSign; (b) Subscriber reduces such tax to the extent possible, giving effect to the applicable Income Tax Convention between the United States and other jurisdictions; and (c) Subscriber furnishes DocuSign with such evidence as the United States taxing authorities may require to claim the credit. Subscriber will pay any additional taxes as are necessary to ensure that the net amounts received and retained by DocuSign after all such taxes are paid are equal to the amounts that DocuSign would have been entitled to in accordance with this Agreement as if the taxes did not exist.

9. TERM AND TERMINATION

9.1 Term. Unless sooner terminated as stated below, and subject to Section 17 with respect to Work Orders (as defined below), the effectiveness of this Agreement will commence upon the Order Start Date and will continue for the term specified on the Order Form (the "Term").

9.2 Termination for Cause. If either party commits a material breach or default in the performance of any of its obligations under this Agreement, then the other party may terminate this Agreement by giving the defaulting party written notice of termination if the material breach or default in performance is not cured within 30 days after the defaulting party receives notice thereof. Without limiting the foregoing, any failure by Subscriber to timely pay to DocuSign any amounts owing under this Agreement will constitute a material breach of this Agreement. If Subscriber fails to timely pay any amounts due for services to be performed by DocuSign, then without limitation to any of its other rights or remedies, DocuSign may suspend performance of such services until it receives all amounts due.

9.3 Post-Termination Obligations. If this Agreement expires or is terminated for any reason: (a) Subscriber will pay to DocuSign any amounts required to be paid under this Agreement that have accrued prior to, and remain unpaid as of, the date of

termination or expiration (including Subscription fees, which become due upon termination of this Agreement as set forth in an Order Form, and any one-time or recurring fees through the end of the billing cycle in which termination occurs); (b) any and all liabilities accrued prior to the effective date of the termination will survive; (c) Subscriber will destroy all copies of DocuSign software, documentation, and materials within five business days of such termination, and immediately thereafter, if requested by DocuSign, provide DocuSign with a written certification signed by an authorized Subscriber representative certifying that all copies of software, documentation, and materials have been destroyed; (d) licenses to use DocuSign software and the provision of DocuSign services will immediately end; and (e) the parties' rights and obligations under Sections 1, 7.4, 9.3, 9.4, 10.3, and 11 through 14 will survive.

9.4 Transition Services. Upon expiration or termination of this Agreement for any reason, at Subscriber's request and at DocuSign's then-current standard professional services rates plus expenses, DocuSign shall provide reasonable transition services for a period not to exceed 90 days to assist Subscriber in moving Subscriber's data to another provider or exporting eContracts to external media. As part of such transition services, DocuSign shall at a minimum transfer, and cause any of its independent contractors to transfer, all data and electronic files associated with the Subscription Service. At its then-current standard professional services rates, DocuSign shall at Subscriber's request further cooperate with Subscriber in the development of a transition plan and shall use reasonable efforts to assist Subscriber and/or another service provider in the transition. DocuSign may at its discretion require advance payment or other adequate security for payment as DocuSign may consider appropriate in connection with or as a condition to the provision of services described in this section.

10. WARRANTIES AND DISCLAIMERS

10.1 DocuSign Warranties. DocuSign represents and warrants that: (a) the Subscription Service as delivered to Subscriber and used in accordance with the Specifications will not infringe on any United States patent, copyright or trade secret; (b) the Subscription Service shall be performed in accordance with the Specifications in their then-current form at the time of the provision of such Subscription Service; (c) any DocuSign Products that are software shall be free of harmful or illicit code, trapdoors, viruses, or other harmful features; (d) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract not involving any consumer will be sufficient under the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. (the "ESIGN Act") to support the validity of such formation, to the extent provided in the ESIGN Act; (e) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract involving a consumer will be sufficient under the ESIGN Act to support the validity of such formation, to the extent provided in the ESIGN Act, so long as and provided that Subscriber complies with all special requirements for consumer eContracts, including and subject to those referenced in Section 2.1(vi) and (vii) above; and (f) DocuSign has implemented information security policies and safeguards to preserve the security, integrity, and confidentiality of Personal Data and to protect against unauthorized access and anticipated threats or hazards thereto, that meet the objectives of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information as set forth in Section 501 (b) of the Gramm-Leach-Bliley Act.

10.2 Mutual Warranties. Each party represents and warrants to the other that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (b) no authorization or approval from any third party is required in connection with such party's execution, delivery, or performance of this Agreement; and (c) the execution, delivery, and performance of this Agreement does not violate the laws of any jurisdiction or the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.

10.3 Disclaimer. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN SECTIONS 10.1 AND 10.2 ABOVE (WHICH ARE NOT APPLICABLE TO CONSULTING SERVICES), DOCUSIGN MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND -- WHETHER EXPRESS, IMPLIED IN FACT OR BY OPERATION OF LAW, OR STATUTORY -- AS TO ANY MATTER WHATSOEVER. DOCUSIGN EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. DOCUSIGN DOES NOT WARRANT THAT THE DOCUSIGN PRODUCTS (INCLUDING CONSULTING SERVICES OR RELATED DELIVERABLES, IF ANY), ARE OR WILL BE ERROR-FREE, WILL MEET SUBSCRIBER'S REQUIREMENTS, OR BE TIMELY OR SECURE. SUBSCRIBER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY.

11. INDEMNIFICATION

11.1 By DocuSign. DocuSign will defend Subscriber, and its employees, directors, agents, and representatives ("Indemnified Party") from any actual or threatened third party claim arising from: (a) any breach by DocuSign of its confidentiality obligations in Section 13, and/or (b) alleged infringement by DocuSign of any third party intellectual property rights (each a "Subscriber Claim").

11.2 By Subscriber. Subscriber will defend DocuSign, and its employees, directors, agents, and representatives ("Indemnified Party") from any actual or threatened third party claim arising from: (a) any breach by Subscriber of its confidentiality obligations in Section 13, and/or (b) alleged infringement by Subscriber of any third party intellectual property rights, and/or (c) the content submitted by any Authorized User or otherwise Processed through Subscriber's Account (each a "DocuSign Claim").

11.3 Procedures. The parties' respective indemnification obligations above are conditioned on: (a) the Indemnified Party gives the Indemnifying Party prompt written notice of the Subscriber Claim or DocuSign Claim (as the case may be, a "Claim"); (b) the Indemnifying Party has full and complete control over the defense and settlement of the Claim; (c) the Indemnified Party provides assistance in connection with the defense and settlement of the Claim as the Indemnifying Party may reasonably request; and (d) the Indemnified Party complies with any settlement or court order made in connection with the Claim. The Indemnifying Party will indemnify the Indemnified Party against: (i) all damages, costs, and attorneys' fees finally awarded against any of them in any Claim under this Section 11; (ii) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by any of them in connection with the defense of the Claim (other than attorneys' fees and costs incurred without the Indemnifying Party's consent after it has accepted defense of such Claim); and (iii) if any Claim arising under this Section 11 is settled by the Indemnifying Party or with its approval, then the Indemnifying Party will pay any amounts to any third party agreed to by the Indemnifying Party in settlement of any such Claims.

12. LIMITATIONS OF LIABILITY

12.1 Disclaimer of Consequential Damages. EXCEPT WITH RESPECT TO INDEMNIFICATION OBLIGATIONS OF SECTION 11, NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, NEITHER PARTY WILL, UNDER ANY CIRCUMSTANCES, BE LIABLE TO THE OTHER PARTY FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTIONS CONTEMPLATED UNDER THIS AGREEMENT (INCLUDING WITH RESPECT TO CONSULTING SERVICES, IF ANY), INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF BUSINESS, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING.

12.2 Cap on Liability. EXCEPT WITH RESPECT TO INDEMNIFICATION OBLIGATIONS OF SECTION 11, UNDER NO CIRCUMSTANCES WILL EITHER PARTY'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, BUT NOT LIMITED TO, WARRANTY CLAIMS AND WITH RESPECT TO CONSULTING SERVICES, IF ANY), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID BY SUBSCRIBER TO DOCUSIGN UNDER THIS AGREEMENT DURING THE 12 MONTHS PRECEDING THE DATE OF THE ACTION OR CLAIM.

12.3 Independent Allocations of Risk. EACH PROVISION OF THIS AGREEMENT THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES REPRESENTS AN AGREED ALLOCATION OF THE RISKS OF THIS AGREEMENT BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY DOCUSIGN TO SUBSCRIBER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS AGREEMENT, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE WARRANTIES IN THIS AGREEMENT HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

13. CONFIDENTIALITY

13.1 "Confidential Information" means any trade secrets or other information of DocuSign or Subscriber, whether of a technical, business, or other nature (including, without limitation, in the case of DocuSign, DocuSign software and related information, and in the case of Subscriber, Personal Data and eContracts), that is disclosed to the other party (the "Recipient"). Confidential Information does not include any information that: (a) was known to Recipient prior to receiving it from the disclosing party; (b) is independently developed by Recipient without use of or reference to any Confidential Information of the other party; (c) is acquired by Recipient from another source that did not receive it in confidence from the other party to this Agreement; or (d) is or becomes part of the public domain through no fault or action of Recipient.

13.2 Restricted Use and Nondisclosure. During and after the Term, Recipient will: (a) use the Confidential Information of the other party solely for the purpose for which it is provided; (b) not disclose such Confidential Information to a third party; and (c) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature.

13.3 Required Disclosure. If Recipient is required by law to disclose Confidential Information of the other party or the terms of this Agreement, Recipient must give prompt written notice of such requirement before such disclosure and assist the disclosing party to obtain where reasonably available an order protecting the Confidential Information from public disclosure.

13.4 Return of Materials. Except for as provided in Section 7.4, upon written request by the disclosing party, Recipient will destroy or deliver to the disclosing party all of the disclosing party's Confidential Information that Recipient may have in its possession or control.

13.5 Ownership. Recipient acknowledges that, as between the parties, all Confidential Information it receives from the disclosing party, including all copies thereof in Recipient's possession or control, in any media, is proprietary to and exclusively owned by the disclosing party. Nothing in this Agreement grants Recipient any right, title or interest in or to any of the disclosing party's Confidential Information. Recipient's incorporation of the disclosing party's Confidential Information into any of its own materials shall not render Confidential Information non-confidential.

13.6 Remedies. Recipient acknowledges that any actual or threatened violation of this confidentiality provision may cause irreparable, non-monetary injury to the disclosing party, the extent of which may be difficult to ascertain, and therefore agrees that the disclosing party shall be entitled to seek injunctive relief in addition to all remedies available to the disclosing party at law and/or in equity. Absent written consent of the disclosing party, the burden of proving that the disclosing party's Confidential Information is not, or is no longer, confidential or a trade secret shall be on the Recipient.

13.7 Existing Obligations. The obligations in this Section 13 are in addition to, and supplement, each party's obligations of confidentiality under applicable law and/or under any nondisclosure or other agreement between the parties.

14. GENERAL

14.1 Relationship. At all times, the parties are independent actors, and are not the agent or representative of the other. This Agreement is not intended to create a joint venture, partnership, or franchise relationship, or give rise to any third party beneficiary. Subscriber must not represent to anyone that Subscriber is an agent of DocuSign or is otherwise authorized to bind or commit DocuSign in any way without DocuSign's prior authorization.

14.2 Assignability. Subscriber may not assign its rights, duties, or obligations under this Agreement without DocuSign's prior written consent. If consent is given, this Agreement will bind Subscriber's successors and assigns. Any attempt by Subscriber to transfer its rights, duties, or obligations under this Agreement except as expressly provided in this Agreement is void. Notwithstanding the foregoing, either party may assign this Agreement to a successor of its business without the other party's consent.

14.3 Nonsolicitation. During the Term of this Agreement and for a period of one year thereafter, Subscriber will not, directly or indirectly, employ or solicit the employment or services of a DocuSign employee or independent contractor without the prior written consent of DocuSign.

14.4 Notices. Any notice required or permitted to be given in accordance with this Agreement will be effective if it is in writing and sent using: (a) the "acknowledge receipt" function of the Subscription Service; (b) by certified or registered mail; or (c) insured courier, to the appropriate party at the address set forth on the Order Form. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notices are deemed given upon receipt if delivered using the Subscription Service, two business days following the date of mailing, or one business day following delivery to a courier.

14.5 Force Majeure. Except for any payment obligations, neither party will be liable for, or be considered to be in breach of or default under this Agreement on account of, any delay or failure to perform as required by this Agreement as a result of any cause or condition beyond such party's reasonable control, so long as such party uses all commercially reasonable efforts to avoid or remove such causes of non-performance or delay.

14.6 Dispute Resolution. In the event of any dispute regarding any right or obligation under this Agreement, the aggrieved party shall notify the other party in a writing describing the dispute ("Notice of Dispute"). Upon receipt of the Notice of Dispute, the parties shall arrange a meeting between their representatives. Over a period not to exceed 10 business days after receipt of Notice of Dispute ("Period"), the parties shall engage in good faith negotiations to resolve such dispute. If the parties' representatives are unable to resolve the dispute at such meetings during the Period, then each party may seek any remedies available to it in law or equity. Notwithstanding the foregoing, either party may seek injunctive relief at any time. Each party hereby irrevocably waives, to the fullest extent permitted by law, any and all right to trial by jury in any legal proceeding arising out of or relating to this Agreement.

14.7 Governing Law. This Agreement will be interpreted, construed, and enforced in all respects in accordance with the local laws of the State of Washington, U.S.A., without reference to its choice of law rules to the contrary. The provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods are expressly excluded and do not apply to this Agreement. Any legal action by Subscriber arising under this Agreement must be initiated within two years after the cause of action arises.

14.8 Waiver. The waiver by either party of any breach of any provision of this Agreement does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with this Agreement will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of this Agreement.

14.9 Severability. If any part of this Agreement is found to be illegal, unenforceable, or invalid, the remaining portions of this Agreement will remain in full force and effect. If any material limitation or restriction on the grant of any license to Subscriber under this Agreement is found to be illegal, unenforceable, or invalid, the license will immediately terminate.

14.10 Counterparts. This Agreement may be executed in any number of identical counterparts, notwithstanding that the parties have not signed the same counterpart, with the same effect as if the parties had signed the same document. All counterparts will be construed as and constitute the same agreement.

14.11 Entire Agreement. This Agreement is the final and complete expression of the agreement between these parties regarding the DocuSign Products. This Agreement supersedes, and the terms of this Agreement govern, all previous oral and written communications regarding these matters. This Agreement may be changed only by a written agreement signed by an authorized agent of both parties.

ADDITIONAL TERMS AND CONDITIONS FOR CONSULTING SERVICES

The following additional terms and conditions apply to Consulting Services, if any, that are made the subject of an Order Form.

15. SERVICES, WORK ORDERS, AND CHANGE ORDERS

15.1 Services. Subject to the terms and conditions of this Agreement, DocuSign will, if ordered as provided hereunder, perform for Subscriber certain Consulting Services.

15.2 Work Orders. The specific details of the Consulting Services to be performed will be determined on a per-project basis, and the details for each project will be described in a Work Order that is executed by both parties (called the "Work Order" for purposes of the Consulting Services). An Order Form that lists a DocuSign standard training or consulting package as a DocuSign Product constitutes a Work Order. Once executed by both parties, each Work Order will be a unique agreement that incorporates the terms of this Agreement and stands alone with respect to all other Order Forms. If there is a conflict between the terms of this Agreement and the terms of a Work Order, the terms of this Agreement will control unless the Work Order states that a specific provision of this Agreement will be superseded by a specific provision of the Work Order.

15.3 Change Orders. Unless otherwise specified in a Work Order, Subscriber may reasonably request in writing that revisions be made with respect to the Consulting Services or deliverables set forth in that Work Order ("Change Order"). If a Change Order recites revisions that materially increase the scope of the Consulting Services or the effort required to deliver deliverables under the applicable Work Order, then within 10 business days after DocuSign's receipt of the Change Order, DocuSign will deliver to Subscriber a written, revised Work Order reflecting DocuSign's reasonable determination of the revised Consulting Services, deliverables, delivery schedule, payment schedule, and adjusted fees or fee estimates, if any, that will apply to the implementation of the revisions. If Subscriber approves the revised Work Order, then the parties will execute it, and upon execution, the revised Work Order will supersede the then-existing Work Order. If Subscriber does not approve the revised Work Order within 10 business days after its receipt by Subscriber, the then-existing Work Order will remain in full force and effect, and DocuSign will have no further obligation with respect to the applicable Change Order.

16. PERFORMANCE OF CONSULTING SERVICES

16.1 Project Management. For each project described in a Work Order, each party will designate a single point of contact within its organization to manage the project ("Project Leader"). The Project Leaders will meet as necessary to manage the Consulting Services to be performed under a Work Order. Disputes will be escalated to more senior executives if the Project Leaders are unable to resolve a problem. DocuSign's Project Leader will provide Subscriber's Project Leader with regular reports on the status of the Consulting Services at least once per month.

16.2 Performance Standard. DocuSign warrants to Subscriber that the Consulting Services will be performed in a good and workmanlike manner in accordance with standard industry practice and the applicable Work Order, including any specifications

in such Work Order. DocuSign will complete the Consulting Services, including the delivery of any deliverables, in accordance with the schedule of times and milestones specified in the Work Order.

16.3 Fees. Unless otherwise specified in a Work Order, Subscriber will pay DocuSign for Consulting Services on a time-and-materials basis at DocuSign's then-current rates and under payment terms described in this Agreement ("Consulting Fees").

16.4 Disclaimer. EXCEPT FOR WARRANTIES PROVIDED HEREIN OR EXPRESSLY IDENTIFIED AS SUCH IN A WORK ORDER, THE CONSULTING SERVICES AND ANY RELATED DELIVERABLES WILL BE PROVIDED AS-IS AND WITHOUT WARRANTY OF ANY KIND. DOCUSIGN EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AS TO ANY AND ALL CONSULTING SERVICES AND RELATED DELIVERABLES.

17. TERM AND TERMINATION OF WORK ORDERS

17.1 Term. Each Work Order is non-cancellable except pursuant to a Change Order, and will commence on the specified effective date and will continue until each party's obligations under the Work Order have been fulfilled or the Work Order is terminated as provided in the Work Order.

17.2 Effect of Termination. If any Work Order is terminated in accordance with this Section 17, then Subscriber will pay to DocuSign any Consulting Fees and all other payment obligations accrued and payable for the Consulting Services performed under the terminated Work Order through the effective date of the termination. If a Work Order is terminated for any reason other than for material breach by DocuSign, Subscriber will pay to DocuSign all Consulting Fees due under the Work Order had the Work Order not been terminated and had the Consulting Services been fully performed in accordance with the schedule then in effect, which amount owing will be evidenced in a final termination invoice to be provided by DocuSign to Subscriber. The amount of Consulting Services Fees specified in such termination invoice from DocuSign will be final and binding on the parties, absent manifest error.

18. PROPRIETARY RIGHTS

18.1 Subscriber Materials. Any materials provided by Subscriber to DocuSign specifically for use by DocuSign in the course of the Consulting Services ("Subscriber Materials") will be used and disclosed solely as required to perform the Consulting Services. As between the parties, Subscriber will continue to own the Subscriber Materials.

18.2 Inventions. Except as expressly set forth to the contrary in a Work Order, all works of authorship, inventions, discoveries, improvements, methods, processes, formulas, designs, techniques, and information: (a) conceived, discovered, developed or otherwise made by DocuSign, solely or in collaboration with others, in the course of performing the Consulting Services; or (b) that form all or part of a deliverable provided as part of the Consulting Services, whether developed as part of the Consulting Services or separately, but excluding Subscriber Materials (as defined in Section 18.1) (collectively, "Inventions"), will be the sole property of DocuSign. Upon and subject to final payment by Subscriber of all amounts owing to DocuSign, DocuSign hereby grants to Subscriber a nonexclusive, perpetual, worldwide, royalty-free license to use, copy, modify, and prepare derivative works of the Inventions solely for purposes of Subscriber's internal business operations only.

MASTER PURCHASE AGREEMENT

This Master Purchase Agreement (this "Agreement") is entered into as of [DATE] (the "Effective Date") by and between FireEye (as defined below) and _____, a _____ corporation, with its principal place of business at _____("Customer"). This Agreement will govern Customer's initial purchase of FireEye Offerings and any future orders by Customer as agreed between the parties in writing. FireEye shall provide its Offerings pursuant to the terms and conditions below. For good and valuable consideration, the parties hereby agree as follows:

Structure and Order of Precedence. This Agreement provides the general terms under which the Customer may use FireEye's various Offerings. The explicit rights for the Customer to use and receive Products, Support Services or Subscriptions or otherwise engage with specific FireEye Offerings are set forth in the applicable Exhibit. In the event of conflict between any of the terms in this Agreement and an Exhibit, the Exhibit shall govern.

GENERAL TERMS APPLICABLE TO ALL FIREEYE OFFERINGS

1. DEFINITIONS.

1.1 "Content Feed" means all intelligence and content feeds associated with Products, which may consist of inbound and outbound feeds that are part of FireEye's Dynamic Threat Intelligence (DTI) Cloud, downloads of Indicators for use with Products, and/or intelligence provided as part of the Advanced Threat Intelligence (ATI) Subscription.

1.2 "Deliverables" means the written reports that are created specifically for Customer as a result of the Professional Services provided hereunder.

1.3 "Documentation" means the user manuals generally provided in writing by FireEye to end users of the Products and Subscriptions in electronic format, as amended from time to time by FireEye.

1.4 "FireEye" means (i) FireEye, Inc., a Delaware corporation with its principal place of business at 1440 McCarthy Blvd., Milpitas, CA, 95035 with respect to Offerings that are shipped to, deployed or rendered inside of North America (including the United States, Mexico, Canada and the Caribbean), Central America and South America (collectively, the "Americas"); or (ii) with respect to all Offerings that are shipped to, deployed or rendered outside of the Americas, FireEye Ireland Limited, a company incorporated under the laws of Ireland with principal place of business at 2 Park Place, City Gate Park, Mahon, Cork, Ireland. FireEye includes the operating divisions Mandiant and iSIGHT.

1.5 "FireEye Materials" means all FireEye proprietary materials, Deliverables, intellectual property related to Products or Subscriptions, (such as all rights in any software incorporated into a Product or Subscription, copyrights, and patent, trade secret and trademark rights related to Products, and screens associated with Products or Subscriptions), Documentation, any hardware and/or software used by FireEye in performing Services or providing Subscriptions, Content Feeds, FireEye's processes and methods (including any forensic investigation processes and methods), Indicators of Compromise, materials distributed by FireEye during Training, and any FireEye templates and/or forms, including report and presentation templates and forms. FireEye Materials does not include Third Party Materials.

1.6 "Indicators of Compromise" or "Indicators" means specifications of anomalies, configurations, or other conditions that FireEye is capable of identifying within an information technology infrastructure, used by FireEye in performing Professional Services and providing Subscriptions.

1.7 "Intellectual Property Rights" means copyrights (including, without limitation, the exclusive right to use, reproduce, modify, distribute, publicly display and publicly perform the copyrighted work), trademark rights (including, without limitation, trade names, trademarks, service marks, and trade dress), patent rights (including, without limitation, the exclusive right to make, use and sell), trade secrets, moral rights, right of publicity, authors' rights, contract and licensing rights, goodwill and all other intellectual property rights as may exist now and/or hereafter come into existence and all renewals and extensions thereof, regardless of whether such rights arise under the law of the United States or any other state, country or jurisdiction.

1.8 "Offerings" means, collectively, Products, Subscriptions, Training, Professional Services and Support Services.

1.9 "Order" means a written purchase order or similar ordering document, signed or submitted to FireEye by Customer and approved by FireEye, under which Customer agrees to purchase Offerings.

1.10 "Products" means the FireEye software and hardware appliances (which may include embedded software or firmware components) as described in Exhibit A to this Agreement.

1.11 "Professional Services" means, collectively, those security consulting services provided by FireEye under a Statement of Work and/or set forth on an Order, which may consist of Product-related services such as deployment, configuration or installation services; proactive security consulting such as penetration testing, vulnerability assessments or compromise assessments; or incident response or other remediative services.

1.12 "Service" or "Services" means the Professional Services, Support Services and Training.

1.13 "Statement of Work" or "SOW" means a mutually agreed-upon document between FireEye and Customer, describing Professional Services, rates and timelines (if applicable) for those Professional Services, and incorporating this Agreement.

1.14 "Subscription" means a service provided by FireEye for a fixed term, under which FireEye provides access to certain features, functionality, and/or information, as described in the applicable Exhibit for each Subscription attached to this Agreement.

1.15 "Support Services" means the Product support and maintenance services provided by FireEye with respect to each Product, and that are described in the applicable Exhibit for each Product attached to this Agreement.

1.16 "Third Party Materials" means software or other components that are licensed to FireEye by third parties for use in FireEye's Offerings.

1.17 "Training" means training in the use of Products, or on security-related topics in general, provided by FireEye.

2. ORDERS AND STATEMENTS OF WORK.

2.1. Orders. Customer may purchase Offerings by submitting an Order. If accepted by FireEye, the "Order Effective Date" will be the date of the Order. All Orders will be governed by this Agreement. For clarity, FireEye will not be obligated to ship any Product, or provide any Services, Training or Subscriptions until Customer has issued a valid Order for those Offerings.

2.2. Statements of Work. Each Statement of Work will incorporate and be governed by this Agreement. The "Statement of Work Effective Date" will be the date both Customer and FireEye have agreed to the Statement of Work, either by executing the Statement of Work or by issuing and accepting an Order for the Professional Services described on the Statement of Work. For clarity, FireEye will not be obligated to perform any Professional Services until a SOW describing those Professional Services has been agreed by both parties or an Order listing those Professional Services has been accepted by FireEye.

3. PAYMENT. Customer agrees to purchase the Offerings for the prices set forth in each Order and/or Statement of Work, as applicable ("Fees"). If Customer purchases through a FireEye partner (such as an authorized reseller or distributor, collectively, "FireEye Partners"), all fees and other procurement and delivery terms shall be agreed between Customer and the applicable partner. If Customer purchases directly from FireEye, Customer will make full payment in the currency specified in FireEye's invoice, without set-off and in immediately available funds, within thirty (30) days of the date of each invoice. All Fees are non-cancelable and non-refundable. All Fees described on an Order will be fully invoiced in advance, unless otherwise agreed by FireEye. Unless otherwise specified in a Statement of Work, all Fees related to Professional Services will be invoiced

fully in advance. Customer shall reimburse FireEye for any and all expenses incurred so long as such expenses are directly attributable to the Services or Subscriptions performed for or provided to Customer. FireEye will provide appropriate vouching documentation for all expenses exceeding $25. If any payment is more than fifteen (15) days late, FireEye may, without limiting any remedies available to FireEye, terminate the applicable Order or Statement of Work or suspend performance until payment is made current. Customer will pay interest on all delinquent amounts at the lesser of 1.5% per month or the maximum rate permitted by applicable law. All Fees are exclusive of all present and future sales, use, excise, value added, goods and services, withholding and other taxes, and all customs duties and tariffs now or hereafter claimed or imposed by any governmental authority upon the Offerings which shall be invoiced to and paid by the Customer. If Customer is required by law to make any deduction or withholding on any payments due to FireEye, Customer will notify FireEye and will pay FireEye any additional amounts necessary to ensure that the net amount FireEye receives, after any deduction or withholding, equals the amount FireEye would have received if no deduction or withholding had been required. Additionally, Customer will provide to FireEye evidence, to the reasonable satisfaction of FireEye, showing that the withheld or deducted amounts have been paid to the relevant governmental authority. For purposes of calculating sales and similar taxes, FireEye will use the address set forth on the Order or Statement of Work, as applicable, as the jurisdiction to which Offerings and shipments are delivered unless Customer has otherwise notified FireEye in writing as of the Order Effective Date or Statement of Work Effective Date, as applicable. Customer will provide tax exemption certificates or direct-pay letters to FireEye on or before the Order Effective Date or Statement of Work Effective Date, as applicable. FireEye reserves the right to increase Fees at any time, although increases in Fees for Subscriptions or Support Services will not go into effect until the next Renewal Subscription Term or Renewal Support Term, as applicable.

4. TITLE AND RISK OF LOSS; INSPECTION. All hardware, including Products and any hardware provided for use with Subscriptions and/or Services, is shipped FOB Origin (FCA) from FireEye's designated manufacturing facility or point of origin, and title to such hardware and the risk of loss of or damage to the hardware shall pass to Customer at time of FireEye's delivery of such hardware to the carrier. FireEye is authorized to designate a carrier pursuant to FireEye's standard shipping practices unless otherwise specified in writing by Customer. Customer must provide written notice to FireEye within five (5) days of delivery of the Products of any non-conformity with the Order, e.g., delivery of the wrong Product or incorrect quantities.

5. TERMS APPLICABLE TO OFFERINGS.

5.1. Products and Support Services. Customer's purchase and use of each Product and Support Services for each Product will be subject to the licenses and terms specific to each Product set forth in Exhibit A.

5.2. Subscriptions. Customer's purchase of and access to each Subscription will be subject to the terms specific to each Subscription set forth in Exhibit B.

5.3. Training. Customer's purchase of Training will be subject to the terms in this Section 5.3. Training delivery dates and location for such Training will be mutually agreed upon by the parties. If an Order does not specify such dates and/or locations, then the parties will mutually agree upon the dates and locations for Training. Customer must request rescheduling of Training no less than two (2) weeks in advance of the scheduled start date. FireEye will use reasonable efforts to reschedule the Training, subject to availability, and Customer will pay any expenses associated with the rescheduling, including any expenses associated with cancelling or changing travel plans. If Customer cancels attendance at a public Training class, Customer must notify FireEye no later than two (2) business days before the date of the Training class. If Customer timely notifies FireEye of the cancellation, FireEye will issue Customer a credit for the amount paid for that public Training class, which Customer may apply toward another public Training class held within one (1) year of the date of the Order on which the cancelled Training class was included. Customer may substitute a named attendee at a public Training class, but Customer will notify FireEye in advance of any such substitution. FireEye reserves the right to refuse admittance to public Training classes to any person, for any reason, and if FireEye refuses admittance, FireEye will refund the amount paid for that person's attendance at the public Training class. FireEye does not refund or credit Fees paid for attendees who do not attend Training classes or who leave before a Training class concludes. If Customer purchases a block of Training hours (for example, 10 hours of Training), then Customer must use those hours within one (1) year of the effective date of the applicable Order. All Training must be scheduled and conducted within one (1) year of the date of the applicable Order for that Training.

5.4. Professional Services.

5.4.1. Deliverables. Subject to Customer's timely payment of applicable fees, and subject to this Agreement and each applicable SOW, Customer shall have a perpetual, non-exclusive, nontransferable, right and license to use, display and reproduce the Deliverables for its internal business purposes. Deliverables may not be shared with any third party other than law enforcement agencies. In no event may Deliverables be used for sales or marketing activities.

5.4.2. Customer-Owned Property. Customer will be and remain, at all times, the sole and exclusive owner of the Customer-Owned Property (including, without limitation, any modification, compilation, derivative work of, and all intellectual property and proprietary rights contained in or pertaining thereto). FireEye will promptly return to Customer all Customer-Owned Property upon the termination or expiration of the applicable Statement of Work or Order, or sooner at Customer's request. "Customer-Owned Property" means any technology, software, algorithms, formulas, techniques or know-how and other tangible and intangible items that were owned by Customer, or developed by or for Customer prior to the SOW Effective Date that are provided by Customer to FireEye for incorporation into or used in connection with the development of the Deliverables or performance of Professional Services.

5.4.3. Customer Responsibilities. If the Services or Subscriptions require the installation and use of FireEye equipment or software, Customer will facilitate the installation and shall provide physical space, electrical power, Internet connectivity and physical access as reasonably determined and communicated by FireEye. Notwithstanding anything to the contrary herein or in any Statement of Work, including confidentiality provisions, if Customer has hired FireEye to perform a PCI DSS Compliance Audit or a PCI investigation, FireEye may provide The Payment Card Industry Security Standards Council, LLC (PCI SSC), card companies and the relevant merchant bank with all Reports of Compliance (ROC) and all related assessment and investigative report documents generated in connection with such work, as required by PCI DSS rules.

5.4.4. Additional Assumptions. (a) estimated Fees for Professional Services do not include any hardware, software, licensing, maintenance or support costs of any FireEye or other third-party product or service suggested by FireEye in the course of performing Professional Services; (b) when FireEye's personnel are performing Professional Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all FireEye personnel; (c) Customer will make available key individuals within the security program that can best help plan and coordinate activities described in the SOW; (d) either party may elect to submit written change requests to the other party proposing changes to the Statement of Work. All changes to the requirements and Statement of Work will be made using agreed-to project change control procedures.

5.5 Evaluations. If Customer receives a Product or Subscription for evaluation purposes ("Evaluation Offerings") then Customer may use the Evaluation Offerings for its own internal evaluation purposes for a period of up to thirty (30) days from the date of receipt of the Evaluation Offerings (the "Evaluation Period"). Customer and FireEye may, upon mutual written agreement (including via email), extend the Evaluation Period. If the Evaluation Offering includes hardware components, Customer will return the hardware within ten (10) days of the end of the Evaluation Period, and if Customer does not return the hardware within this period, Customer shall be invoiced for the then-current list price for the applicable Evaluation Offering. Customer acknowledges that title to hardware components of Evaluation Offerings remains with FireEye at all times, and that Evaluation Offerings may be used and/or refurbished units. If the Evaluation Offering does not include hardware components, Evaluator must delete all software and other components (including Documentation) related to the Evaluation Offering at the end of the Evaluation Period, and confirm those deletions in writing to FireEye, or the Evaluator shall be invoiced for the then-current list price for the Evaluation Offering. If the Evaluation Offering is a Subscription, Evaluator understands that FireEye may disable access to the Subscription automatically at the end of the Evaluation Period, without notice to Evaluator. EVALUATION OFFERINGS ARE PROVIDED "AS IS", AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, FIREEYE DISCLAIMS ALL WARRANTIES RELATING TO THE EVALUATION OFFERINGS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. INTELLECTUAL PROPERTY

6.1. Ownership of FireEye Materials; Restrictions. All Intellectual Property Rights in FireEye Materials, Products, Deliverables, Documentation, and Subscriptions belong exclusively to FireEye and its licensors. Customer will not (and will not allow any third party to): (i) disassemble, decompile, reverse compile, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of any FireEye Materials (except to the limited extent that applicable law prohibits reverse engineering restrictions); (ii) sell, resell, distribute, sublicense or otherwise transfer, the FireEye Materials, or make the functionality of the FireEye Materials available to any other party through any means (unless otherwise FireEye has provided prior written consent), (iii) without the express prior written consent of FireEye, conduct any benchmarking or comparative study or analysis involving the FireEye Materials ("Benchmarking") for any reason or purpose except, to the limited extent absolutely necessary, to determine the suitability of Products or Subscriptions to interoperate with Customer's internal computer systems; (iv) disclose or publish to any third party any Benchmarking or any other information related thereto; (v) use the FireEye Materials or any Benchmarking in connection with the development of products, services or subscriptions that compete with the FireEye Materials; or (vi) reproduce, alter, modify or create derivatives of the FireEye Materials. Between Customer and FireEye, FireEye shall retain all rights and title in and to any Indicators of Compromise FireEye developed by or for FireEye in the course of providing Subscriptions or performing Services.

6.2. Third Party Materials. Customer acknowledges that Products and Subscriptions may include Third Party Materials. FireEye represents that these Third Party Materials will not diminish the license rights provided herein or limit Customer's ability to use the Products and Subscriptions in accordance with the applicable Documentation, and neither the inclusion of Third Party Materials in any Product or Subscription or use of Third Party Materials in performance of Services will create any obligation on the part of Customer to license Customer's software or products under any open source or similar license.

7. WARRANTIES.

7.1. Product Warranty. FireEye warrants to Customer that during the one (1) year period following the shipment of the Products, the Products will perform substantially in accordance with the applicable Documentation. The warranty stated in this Section 7.1 shall not apply if the Product has: (i) been subjected to abuse, misuse, neglect, negligence, accident, improper testing, improper installation, improper storage, improper handling or use contrary to any instructions issued by FireEye; (ii) been repaired or altered by persons other than FireEye; (iii) not been installed, operated, repaired and maintained in accordance with the Documentation; or (iv) been used with any third party software or hardware which has not been previously approved in writing by FireEye. If during the one-year Product warranty period: (a) FireEye is notified promptly in writing upon discovery of any error in a Product, including a detailed description of such alleged error; (b) such Product is returned, transportation charges prepaid, to FireEye's designated manufacturing facility in accordance with FireEye's then-current return procedures, as set forth by FireEye from time to time; and (c) FireEye's inspections and tests determine that the Product contains errors and has not been subjected to any of the conditions set forth in 7.1(i)-(iv) above, then, as Customer's sole remedy and FireEye's sole obligation under the foregoing warranty, FireEye shall, at FireEye's option, repair or replace without charge such Product. Any Product that has either been repaired or replaced under this warranty shall have warranty coverage for the remaining warranty period. Replacement parts used in the repair of a Product may be new or equivalent to new.

7.2. Services Warranty. FireEye warrants to Customer that Services will be performed in a professional manner in accordance with industry standards for like services. If Customer believes the warranty stated in this Section has been breached, Customer must notify FireEye of the breach no later than thirty (30) days following the date the Services were performed, and FireEye will promptly correct or re-perform the Services, at FireEye's expense.

7.3. Subscription Warranty. FireEye warrants to Customer the Subscriptions will be provided in a professional manner in accordance with industry standards for similar subscriptions. If Customer believes the warranty stated in this Section has been breached, Customer must notify FireEye of the breach no later than thirty (30) days following the date the warranty was allegedly breached, and FireEye will promptly correct the non-conformity, at FireEye's expense.

7.4. Remedies Exclusive. Except for any Service Level Credits described in Exhibit B, the remedies stated in Sections 7.1-7.3 above are the sole remedies, and FireEye's sole obligation, with respect to Products, Subscriptions and Services that fail to comply with the foregoing warranties.

7.5. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH HEREIN, ALL PRODUCTS, SUBSCRIPTIONS, FIREEYE MATERIALS, DELIVERABLES AND SERVICES ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY WARRANTY WHATSOEVER. FIREEYE AND ITS SUPPLIERS EXPRESSLY DISCLAIM, TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, ALL WARRANTIES, EXPRESS, IMPLIED AND STATUTORY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. FIREEYE ALSO MAKES NO WARRANTY REGARDING NONINTERRUPTION OF USE OR FREEDOM FROM BUGS, AND MAKES NO WARRANTY THAT PRODUCTS, FIREEYE MATERIALS, DELIVERABLES, SERVICES OR SUBSCRIPTIONS WILL BE ERROR-FREE.

8. INFRINGEMENT INDEMNITY.

8.1. FireEye shall defend Customer, and its officers, directors and employees, against any third party action alleging that the FireEye Materials infringes a valid U.S. patent or copyright issued as of the date of delivery or performance, as applicable, and FireEye shall pay all settlements entered into, and all final judgments and costs (including reasonable attorneys' fees) finally awarded against such party in connection with such action. If the FireEye Materials, or parts thereof, become, or in FireEye's opinion may become, the subject of an infringement claim, FireEye may, at its option: (i) procure for Customer the right to continue using the applicable FireEye Materials; (ii) modify or replace such FireEye Materials with a substantially equivalent non-infringing FireEye Materials; or (iii) require the return of such FireEye Materials or cease providing affected Product, Subscriptions, Deliverables or Services, and refund to Customer, with respect to Products, a pro-rata portion of the purchase price of such Products based on a three-year straight line amortization of the purchase price, and with respect to Subscriptions, a portion of any pre-paid Fees for such Subscriptions, pro rated for any unused Subscription Term, and with respect to Services, any pre-paid Fees for Services that have not been delivered. THIS SECTION 8.1 STATES THE ENTIRE LIABILITY OF FIREEYE AND CUSTOMER'S SOLE REMEDY WITH RESPECT TO ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS BY THE OFFERINGS, FIREEYE MATERIALS, OR DELIVERABLES.

8.2. FireEye shall have no indemnification obligations with respect to any action arising out of: (i) the use of any Product, Subscription, Deliverable, or Service, or any part thereof, in combination with software or other products not supplied by FireEye; (ii) any modification of the Products, Subscriptions, Deliverables, or Services not performed or expressly authorized by FireEye; or (iii) the use of any the Products, Subscriptions, Deliverables, or Services other than in accordance with this Agreement and applicable Documentation.

8.3. The indemnification obligations shall be subject to Customer: (i) notifying FireEye within ten (10) days of receiving notice of any threat or claim in writing of such action; (ii) giving FireEye exclusive control and authority over the defense or settlement of such action; (iii) not entering into any settlement or compromise of any such action without FireEye's prior written consent; and (iv) providing reasonable assistance requested by FireEye.

9. LIMITATION OF LIABILITY.

9.1. Consequential Damages Waiver. EXCEPT FOR LIABILITY ARISING UNDER A BREACH OF ANY INTELLECTUAL PROPERTY RIGHT OF FIREEYE, OR THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 8 (INFRINGEMENT INDEMNITY), IN NO EVENT WILL FIREEYE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS AND LOST SAVINGS, HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT FIREEYE WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

9.2. Limitation of Monetary Damages. EXCEPT FOR LIABILITY ARISING UNDER A BREACH OF ANY INTELLECTUAL PROPERTY RIGHT OF FIREEYE, PAYMENT OBLIGATIONS OF CUSTOMER, AND THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 8 (INFRINGEMENT INDEMNITY), AND NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT OR ANY ORDER OR STATEMENT OF WORK, FIREEYE'S TOTAL LIABILITY ARISING OUT OF THIS AGREEMENT, THE OFFERINGS, THE FIREEYE IP AND DELIVERABLES SHALL BE LIMITED TO THE TOTAL AMOUNTS

RECEIVED BY FIREEYE FOR THE RELEVANT OFFERINGS DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST OCCURRENCE OF THE EVENTS GIVING RISE TO SUCH LIABILITY.

9.3. Applicability. THE LIMITATIONS AND EXCLUSIONS CONTAINED HEREIN WILL APPLY ONLY TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, AND NOTHING HEREIN PURPORTS TO LIMIT EITHER PARTY'S LIABILITY IN A MANNER THAT WOULD BE UNENFORCEABLE OR VOID AS AGAINST PUBLIC POLICY IN THE APPLICABLE JURISDICTION.

9.4 SAFETY Act. FireEye and Customer hereby mutually waive and release each other from any and all liabilities relating to any claims for losses or damages of any kind (including, but not limited to, business interruption losses) arising out of an Act of Terrorism as defined by the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 ("SAFETY Act")(6 U.S.C. §§ 441-444). FireEye and Customer further agree to be solely responsible to the full extent of any and all losses they may sustain, or for any and all losses their respective employees, officers, or agents may sustain, resulting from an Act of Terrorism as defined by 6 U.S.C. §§ 441-444 when FireEye's Multi-Vector Virtual Execution Engine and any subscriptions, cloud services platform or associated services (the "Qualified Anti-Terrorism Technology") are utilized in defense against, response to, or recovery from an Act of Terrorism.

10. Export Control; Anti-Corruption; U.S. Government Restricted Rights.

10.1. Export Control. Export Control. Each party represents and warrants that it shall comply with all laws and regulations applicable to it with respect to the Offerings. Customer further acknowledges and agrees that the Products and FireEye Materials may be subject to restrictions and controls imposed by the United States Export Administration Act, the regulations thereunder, as well as European Union ("EU") or National export control laws and obligations and similar laws in other jurisdictions. Customer agrees to comply with all applicable export and re-export control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State. Specifically, Customer covenants that it shall not, directly or indirectly, sell, export, reexport, transfer, divert, or otherwise dispose of any Products, FireEye Materials, or technology (including products derived from or based on such technology) received from FireEye under this Agreement to any destination, entity, or person prohibited by the laws or regulations of the United States and the EU, without obtaining prior authorization from the competent government authorities as required by those laws and regulations. These prohibitions include, but are not limited to the following: (i) the Products and FireEye Materials cannot be exported or re-exported to any countries embargoed by the United States (currently including Cuba, Iran, North Korea, Sudan or Syria) which includes nationals of these countries employed by Customer; (ii) the Products and FireEye Materials cannot be exported or re-exported for military use in country group 'b' prior to valid 'export license' or valid 'license exception'; and (iii) the Products and FireEye Materials cannot be used for any prohibited end uses including any "nuclear, biological or chemical weapon related activities."; and (iv) the Products and FireEye Materials will not be re-exported or otherwise sold or transferred if it is known or suspected that they are intended or likely to be used for such purposes. Customer agrees to notify FireEye of any suspicious activities by any employee related to the Products. Customer agrees to indemnify, to the fullest extent permitted by law, FireEye from and against any fines or penalties that may arise as a result of Customer's breach of this provision. This export control clause shall survive termination or cancellation of any Orders.

10.2. Anticorruption Laws. Each Party acknowledges that it is familiar with and understands the provisions of the U.S. Foreign Corrupt Practices Act ("the FCPA") and the U.K. Bribery Act of 2010 ("UKBA") and agrees to comply with its terms as well as any provisions of local law related thereto. Each party further understands the provisions relating to the FCPA and UKBA's prohibitions regarding the payment or giving of anything of value, including but not limited to payments, gifts, travel, entertainment and meals, either directly or indirectly, to an official of a foreign government or political party for the purpose of influencing an act or decision in his or her official capacity or inducing the official to use his or her party's influence with that government, to obtain or retain business involving the Offering. Each Party agrees to not violate or knowingly let anyone violate the FCPA or UKBA, and Each Party agrees that no payment it makes will constitute a bribe, influence payment, kickback, rebate, or other payment that violates the FCPA, the UKBA, or any other applicable anticorruption or anti-bribery law.

10.3. U.S. Government Restricted Rights. The Offerings, Deliverables and Documentation are "commercial items", "commercial computer software" and "commercial computer software documentation," pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. All Offerings and FireEye Materials are and were developed solely at private expense. Any use, modification, reproduction, release, performance, display or disclosure of the Offerings, FireEye Materials and Documentation by the United States Government shall be governed solely by the this Agreement and shall be prohibited except to the extent expressly permitted by this Agreement.

11. CONFIDENTIAL INFORMATION.

11.1. Confidential Information. "Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is: (i) identified as confidential at the time of disclosure by the disclosing party ("Discloser"); or (ii) disclosed under circumstances that would indicate to a reasonable person that the information should be treated as confidential by the party receiving such information ("Recipient"). The terms of any commercial transaction between the parties (including pricing related to the Offerings) shall be considered Confidential Information.

11.2. Maintenance of Confidentiality. Each party agrees that it shall: (i) take reasonable measures to protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the Recipient uses to protect its own confidential information of a like nature; (ii) limit disclosure to those persons within Recipient's organization with a need to know and who have previously agreed in writing, prior to receipt of Confidential Information either as a condition of their employment or in order to obtain the Confidential Information, to obligations similar to the provisions hereof; (iii) not copy, reverse engineer, disassemble, create any works from, or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and/or which are provided to the party hereunder; and (iv) comply with, and obtain all required authorizations arising from, all U.S. and other applicable export control laws or regulations.. Confidential Information shall not be used or reproduced in any form except as required to accomplish the purposes and intent of an Order or Statement of Work. Any reproduction of Confidential Information shall be the property of Discloser and shall contain any and all notices of confidentiality contained on the original Confidential Information.

11.3. Exceptions. The parties agree that the foregoing shall not apply to any information that Recipient can evidence: (i) is or becomes publicly known and made generally available through no improper action or inaction of Recipient; (ii) was already in its possession or known by it prior to disclosure by Discloser to Recipient; (iii) is independently developed by Recipient without use of or reference to any Confidential Information; or (iv) was rightfully disclosed to it by, or obtained from, a third party. Recipient may make disclosures required by law or court order provided that Recipient: (a) uses diligent efforts to limit disclosure and to obtain, if possible, confidential treatment or a protective order; (b) has given prompt advance notice to Discloser of such required disclosure; and (c) has allowed Discloser to participate in the proceedings.

11.4. Injunctive Relief. Each party will retain all right, title and interest to such party's Confidential Information. The parties acknowledge that a violation of the Recipient's obligations with respect to Confidential Information may cause irreparable harm to the Discloser for which a remedy at law would be inadequate. Therefore, in addition to any and all remedies available at law, Discloser shall be entitled to seek an injunction or other equitable remedies in all legal proceedings in the event of any threatened or actual violation of any or all of the provisions hereof.

11.5. Return of Confidential Information. Within thirty (30) days after the date when all Orders and SOWs have expired or been terminated, or after any request for return of Confidential Information, each party will return to the other party or destroy all of such other party's Confidential Information, at such other party's discretion, and, upon request, provide such other party with an officer's certificate attesting to such return and/or destruction, as appropriate.

11.6. Privacy. If FireEye is a data processor under this Agreement, further to the provisions of Article 17 and 25 of the EU Data Protection Directive EU (Directive 95/46/EC), FireEye agrees that it will:

11.6.1 only deal with and process personal data controlled by Customer in compliance with, and subject to, the instructions received from Customer and in compliance with this Agreement and will not use or process the personal data for any other purpose whatever;

11.6.2 adopt and maintain appropriate (including organizational and technical) security measures in dealing with Customer's personal data in order to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing; and

11.6.3 take all reasonable steps to ensure that (i) persons employed by it, and (ii) other persons engaged at its place of work, are aware of and comply with applicable data privacy laws and regulations.

11.6.4 FireEye may process or otherwise transfer any personal information in or to any country outside the European Economic Area or any country not deemed adequate by the European Commission pursuant to Article 25(6) to the extent necessary for the provision of the Offerings. If required, FireEye will enter into the EU Standard Contractual Clauses as approved by the European Commission for ensuring an adequate level of data protection in respect of the personal information that will be processed or transferred.

12. TERM AND TERMINATION.

12.1. Term.

12.1.1 Products. Products will be licensed according to the applicable terms in Exhibit A, for the period of time stated on the Order (e.g., if the Order lists a Product as being provided for "3Y," the license for that Product is provided for three years from the date of the Order). If no period of time is stated on the Order, then the Product is licensed perpetually, unless otherwise terminated as set forth herein.

12.1.2 Support Services. Support Services will begin ten (10) days from the date of shipment of the associated Product and continue for the period of time stated on the Order("Initial Support Term"). Unless otherwise stated on the Order, the Support Services will automatically renew for additional periods of one (1) year each (each, a "Renewal Support Term" and together with the Initial Support Term, the "Support Term"), unless either party notifies the other of its intention not to renew Support Services at least sixty (60) days prior to the expiration of the then-current Support Term. Customer may terminate Support at any time, for convenience, on thirty (30) days' written notice to FireEye. If Customer terminates Support Services for convenience before the end of the then-current Support Term, Customer will pay any remaining fees owing for the remainder of the then-current Support Term within thirty (30) days of the effective date of termination.

12.1.3 Subscriptions. The term of each Subscription will begin on the Order Effective Date and will continue in effect for the period of time stated in the Order ("Initial Subscription Term"). Unless otherwise stated on the Order, the Subscription will automatically renew after its Initial Subscription Term for additional periods of one (1) year each (each, a "Renewal Subscription Term" and together with the Initial Subscription Term, the "Subscription Term"), unless either party notifies the other of its intention not to renew that Subscription at least sixty (60) days prior to the expiration of the then-current Subscription Term. Customer may terminate a Subscription at any time, for convenience, on thirty (30) days' written notice to FireEye. If Customer terminates a Subscription for convenience before the end of the then-current Subscription Term, Customer will pay any remaining fees owing for the remainder of the then-current Subscription Term within thirty (30) days of the effective date of termination.

12.1.4 Professional Services; Statements of Work. Professional Services described on an Order will be provided at mutually agreed-upon times, and will continue until complete, unless otherwise terminated as set forth herein. The term of each SOW will be as set forth in that SOW. If no term is expressed in an SOW, then the term of that SOW will begin on the SOW Effective Date and continue until the Professional Services described in that SOW are complete or the SOW is earlier terminated as set forth herein. Unless otherwise stated in a SOW, Customer may terminate a SOW at any time for convenience by giving FireEye at least thirty (30) days' written notice of its intent to terminate the SOW. If Customer terminates an SOW for convenience as set forth in this Section, Customer will pay any amounts owing for Professional Services and Deliverables provided under that SOW up to and including the date of termination. Customer may request that FireEye suspend performing Professional Services during the term of a Statement of Work, and FireEye will suspend such Professional Services within 24 hours of Customer's request. Customer acknowledges that any such suspension will not affect Customer's obligation to pay fees for Professional Services rendered through the date of suspension, and that

resumption of Professional Services may be delayed if FireEye redeploys personnel to other engagements during the period of suspension.

12.2. Termination for Material Breach. Either party may terminate any Order or any SOW upon written notice of a material breach of the applicable Order or SOW by the other party as provided below, subject to a thirty (30) day cure period ("Cure Period"). If the breaching party has failed to cure the breach within the Cure Period after the receipt by the breaching party of written notice of such breach, the non-breaching party may give a second notice to the breaching party terminating the applicable Order or SOW. Termination of any particular Order or SOW under this Section will not be deemed a termination of any other Order or SOW, unless the notice of termination states that another Order or SOW is also terminated. Notwithstanding the foregoing, the Cure Period applicable to a breach by Customer of any payment obligations under any Order or any SOW will be fifteen (15) days. Notwithstanding the foregoing, this Agreement shall terminate automatically in the event Customer has breached any license restriction and, in FireEye's determination, that breach cannot be adequately cured within the Cure Period.

12.3. Effect of Termination. Termination or expiration of any Order or SOW will not be deemed a termination or expiration of any other Orders or SOWs in effect as of the date of termination or expiration, and this Agreement will continue to govern and be effective as to those outstanding Orders and SOWs until those Orders and SOWs have expired or terminated by their own terms or as set forth herein. The provisions of Section 3 (Payment), Section 6 (Intellectual Property), Section 7.5 (Disclaimer of Warranties), 9 (Limitation of Liability), 10 (Export Control; Anti-Corruption; U.S. Government Restricted Rights), 12 (Confidential Information), and 13 (Miscellaneous), and all accrued payment obligations, shall survive the termination of all Orders and SOWs and the relationship between FireEye and Customer.

13. MISCELLANEOUS.

13.1. Assignment. Customer may not assign any Order or Statement of Work, or any rights or obligations thereunder, in whole or in part, without FireEye's prior written consent, and any such assignment or transfer shall be null and void. FireEye shall have the right to assign all or part of an Order or Statement of Work without Customer's approval. Subject to the foregoing, each Order and Statement of Work shall be binding on and inure to the benefit of the parties' respective successors and permitted assigns.

13.2. Entire Agreement. This Agreement along with any Order, Statement of Work and the Exhibits attached hereto is the entire agreement of the parties with respect to the Offerings and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter thereof. FireEye does not accept, expressly or impliedly and FireEye hereby rejects and deems deleted any additional or different terms or conditions that Customer presents, including, but not limited to, any terms or conditions contained or referenced in any order, acceptance, acknowledgement, or other document, or established by trade usage or prior course of dealing. This Agreement may be amended only in writing signed by authorized representatives of both parties.

13.3. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events, which occur after the signing of this Agreement and which are beyond the reasonable control of the parties, such as strikes, blockade, war, terrorism, riots, natural disasters, refusal of license by the government or other governmental agencies, in so far as such an event prevents or delays the affected party from fulfilling its obligations and such party is not able to prevent or remove the force majeure at reasonable cost.

13.4. Governing Law. This Agreement shall be deemed to have been made in, and shall be construed pursuant to the laws of the State of California and the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods or the Uniform Computer Information Transactions Act. Any legal suit, action or proceeding arising out of or relating to the Offerings, the FireEye Materials, this Agreement, an Order or a Statement of Work will be commenced exclusively in a federal court in the Northern District of California or in state court in Santa Clara County, California, and each party hereto irrevocably submits to the jurisdiction and venue of any such court in any such suit, action or proceeding.

13.5. Independent Contractors. The parties are independent contractors. Nothing in this Agreement, any Order or any Statement of Work shall be construed to create a partnership, joint venture or agency relationship between the parties. Customer shall make no representations or warranties on behalf of FireEye.

13.6. Language. This Agreement and each Order and Statement of Work are in the English language only, which shall be controlling in all respects. All communications, notices, and Documentation to be furnished hereunder shall be in the English language only.

13.7. Notices. All notices required to be sent hereunder shall be in writing, addressed to receiving party's current business contact, if known, with a cc: to the General Counsel/Legal Department of the receiving party, and sent to the party's address as listed in this Agreement, or as updated by either party by written notice. Notices shall be effective upon receipt and shall be deemed to be received as follows: (i) if personally delivered by courier, when delivered; or (ii) if mailed by first class mail, or the local equivalent, on the fifth business day after posting with the proper address.

13.8. Severability. If any provision of this Agreement is held to be illegal, invalid or unenforceable under the laws of any jurisdiction, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect.

13.9. Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.10. Waiver. The waiver of a breach of any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach.

13.11. Equal Opportunity. FireEye is committed to the provisions outlined in the Equal Opportunity Clauses of Executive Order 11246, the Rehabilitation Act of 1973, the Vietnam Era Veterans Readjustment Act of 1974, the Jobs for Veterans Act of 2003, as well as any other regulations pertaining to these orders.

Wherefore, the parties have caused this Master Purchase Agreement to be executed as of the Effective Date.

FIREEYE, INC.

Signature: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____

FIREEYE IRELAND LIMITED

Signature**:** _____

Name: _____

Title: _____

Date: _____

EXHIBIT A
PRODUCT LICENSE AND SUPPORT TERMS
(FIREEYE NX, EX, AX, PX, FX, HX, SECURITY ORCHESTRATOR™, MVX SMART GRID, AND CENTRAL MANAGEMENT SERIES (CMS) PRODUCTS)

The following terms apply to the FireEye NX, EX, AX, PX, FX, HX, Security Orchestrator, MVX Smart Grid, and Central Management Series (CMS) Products, including any add-on features such as FireEye Advanced Threat Intelligence (ATI).

1. Grant of License and Restrictions. Subject to the terms hereof, payment of all fees, and any applicable user/use limitations, FireEye grants Customer a personal, perpetual, nonsublicensable, nonexclusive, right to use the Product, in accordance with the Agreement and this Exhibit A. Customer will maintain the copyright notice and any other notices that appear on the Product, including any interfaces related to the Product. With respect to the FireEye HX Series Product, Customer may install the "agent" software component of the Product on the number of Nodes stated on the applicable Order. With respect to the FireEye EX Series Product, Customer may use the Product in connection with the number of attached URL engines (i.e., email accounts) ("Attached URL Engines") stated on the applicable Order. FireEye reserves the right to audit Customer's use of the Product to ensure compliance with this Agreement. "Nodes" are endpoint computing devices owned or controlled by Customer (such as laptops, workstations, and servers), on which Customer installs the agent software. Updates, preview features, Content Feeds and/or Support Services are not necessarily provided with the Software, may require additional payment or include additional terms and conditions, and may be provided on a "preview" basis for a limited period at no additional charge but then licensed for an additional fee at a later date. Customer acknowledges that Third Party Software distributed with the Products may be subject to separate license terms, and specifically, if the Oracle™ Java® software is included within the Product, that software is subject to the license found at http://www.oracle.com/technetwork/java/javase/terms/license/index.html.

2. Content Feeds. Subject to Customer's payment in full of all associated fees for the applicable FireEye Content Feed, as set forth on the applicable Order, FireEye shall grant a limited, non-exclusive, personal, non-transferable, non-sublicenseable right to use the Content Feed as set forth in the Documentation for the applicable Product, for Customer's internal business purposes during the active Support Term for the applicable Product. FireEye shall not disclose to any third party any personally identifiable data or Customer Confidential Information in connection with the Content Feed unless expressly authorized to do so by Customer. The Content Feeds available to the Customer with respect to the Products may include:

2.1 FireEye Dynamic Threat Intelligence™ (DTI™) – The DTI Content Feed (currently available only for customers who have purchased the FireEye NX, EX, AX, HX or FX Product) provides continual, updated information to the Product about threats.

2.2. FireEye Advanced Threat Intelligence™ (ATI™) – The ATI Content Feed (currently available only for customers who have purchased the FireEye NX Product) provides contextual information about malware detected in Customer's environment, such as information regarding threat groups associated with certain malware, industry verticals in which FireEye has observed certain threat groups operate and in which certain malware is used, and relative frequency of observation of various threats and malware.

3. Support Services. Subject to Customer's payment in full of all associated fees for FireEye Support Services, FireEye shall provide Support Services for the Products as set forth in Exhibit C, as may be updated by FireEye in its discretion.

EXHIBIT B
SUBSCRIPTION TERMS

EXHIBIT B-1
SUBSCRIPTION TERMS FOR FIREEYE AS A SERVICE (FAAS) – CONTINUOUS PROTECTION

The following terms govern the FireEye as a Service (FaaS) – Continuous Protection (CP) Subscription.

1 Definitions.

1.1 **"Alert"** means, individually and collectively, APT Alerts, High Priority Alerts, and Low Priority Alerts.

1.2 "**APT Alert**" means (a) with respect to Products other than HX, an alert generated by a Product, that is identified by the Product as being associated with a "targeted threat," which means advanced persistent threat (APT) actors or APT activity; (b) with respect to the HX Product, an alert designated by HX as XPLT, EXC, or PRE, that is triggered by a FireEye standard Indicator; and (c) with respect to the TAP Subscription, an "APT Alert" means a TAP Alert designated as an "APT Alert" in the table in Section 1.11 below.

1.3 "**APT Only Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of APT Alert. If Customer purchases the APT Only Service, FireEye will provide FaaS Reports and monitoring of only APT Alerts, and not any other Alerts.

1.4 "**Covered System**" means (i) a computing device (to the extent supported by FireEye) that Customer specifies as within the scope of the CP Subscription, and if the Customer has purchased the HX Product, on which a software agent has been installed to support CP Subscription delivery, or (ii) a computing device (to the extent supported by FireEye) whose network traffic is observable to support CP Subscription delivery; (iii) with respect to ETP Subscriptions, mailboxes monitored to support CP Subscription delivery; or (iv) any computing device that both Customer and FireEye agree is within scope of the CP Subscription.

1.5 "**Full Coverage Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of all Alerts, regardless of the severity level of the Alert as classified by the Product.

1.6 "**High Priority Alert Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of High Priority Alerts and APT Alerts.

1.7 "**FaaS Reports**" means the written reports relating to Alerts that FireEye creates and makes available to Customer through the CP Subscription.

1.8 "**High Priority Alert**" means (a) with respect to Products other than HX and FX, an alert generated by that Product that is classified by that Product as severity level "critical" or "major"; (b) with respect to the FX Product, any alert generated by the FX Product, including APT Alerts; and (c) with respect to a TAP subscription, a TAP Alert designated as a "High Priority Alert" in the table in Section 1.11 below.

1.9 "**Low Priority Alert**" means an alert generated by a Product or TAP Subscription (as applicable) that is not an APT Alert or a High Priority Alert.

1.10 "**Nodes**" or "**Node Band**" refers to number of Covered Systems within the Customer environment, which is reflected on the Subscription Order.

1.11 "**TAP Alert**" means an alert generated by the TAP Subscription, with a severity level assigned by the TAP Subscription (e.g., "Critical," "High," "Medium"). TAP Alerts are investigated and reported on as "APT Alerts" and "High Priority Alerts" as shown in the table below, depending on the TAP Rule Pack that invoked the TAP Alert:

FireEye Rule Pack	APT Alerts	High Priority Alerts
Application Detection		
Cloud Infrastructure		
Commodity Malware		All

Current Events	Critical, High	Critical, High
DTI Rules		All
Exploit Kits		All
FTP		
Industrial Control Systems	Critical, High, Medium	Critical, High, Medium
Intel Match	Critical, High, Medium	Critical, High, Medium
Linux		Critical, High
Malware Methodology		Critical, High
Phishing	Critical High	Critical, High
Point of Sale	All	All
Security Tools		Critical, High, Medium
Targeted Malware	All	All
Vendor – FireEye		
Vulnerability		Critical, High, Medium
Web Application Attacks		Critical, High, Medium
Windows		Critical, High

1.13 "**TAP Rule Packs**" means a predefined set of criteria that identifies suspicious events or threats based on the associated rule type within the TAP Subscription.

2 **Scope of FaaS – Continuous Protection (CP) Subscription**. During the Subscription Term, FireEye will provide the CP Subscription as set forth in this Section 2, according to the Subscription level purchased by Customer as set forth in the Subscription Order. If the Subscription Order does not specify the Subscription lvel purchased, then Customer will be deemed to have purchased the APT Only Service. All services Customer requests that are not described in this Section 2 will be performed at mutually agreed upon rates as set forth in Statements of Work. Unless otherwise specified, the CP Subscription is provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. The CP Subscription is available for the number of Nodes purchased (available for Customers who have purchased the FireEye NX, FX, or EX Product or the ETP or TAP Subscription). If the number of Nodes exceeds the amount reflected in the Subscription Order by more than ten percent (10%), FireEye will notify Customer in writing, and will issue an invoice for the next higher Node Band at FireEye's then-current rates pro-rated for the remaining portion of the then-current Subscription Term.

2.1 Event Analysis.

(a) Time to Begin Analysis. FireEye will begin analysis of an Alert within the times set forth in the table below, calculated from the time the Alert was generated by the Product or TAP Subscription (as applicable).

(b) Alerts Investigated. FireEye will investigate and report on the Alerts that correspond with the Subscription level the Customer purchased. If the Customer purchased the APT Only Service, FireEye will investigate and report on only APT Alerts. If the Customer purchased the High Priority Alerts Service, FireEye will investigate and report on only High Priority Alerts and APT Alerts. If the Customer purchased the All Alerts Service, FireEye will investigate and report on APT Alerts, High Priority Alerts, and Low Priority Alerts. FireEye has no obligation to investigate and report on Alerts that fall outside the purchased Subscription level.

(c) Initial Investigation. FireEye analysts will perform an initial analysis of the Customer's Covered Systems to determine if the Alert is a true or false positive, benign or suspicious activity.

(d) FaaS Reports. If FireEye's investigation determines that the Alert indicates a true compromise, FireEye will publish a FaaS Report to the FaaS Portal within one (1) hour of the time FireEye makes that determination. Regardless of whether FireEye's investigation determines that an Alert indicates a true compromise, FireEye will publish a FaaS Report on the Alert to the FaaS Portal within the times set forth in the table

below, based on the classification of the Alert (APT Alert, High Priority Alert, Low Priority Alert). Customer acknowledges that in some cases, when FireEye's investigation is not complete, a FaaS Report may provide only an update of current status of the Alert investigation.

Alerts Investigated (Level of Service)			**FaaS Alert Classification**	**Time to Begin Investigation (from time Product or TAP Subscription generates Alert)**	**Time to Publish FaaS Report (from time FireEye validates actual compromise)**	**Time to Publish FaaS Report (when no validation of actual compromise; from time Product or TAP Subscription generates Alert)**
APT Only Service	**High Priority Alerts Service**	**Full Coverage Service**				
Yes	Yes	Yes	APT Alert	1 hours	1 hour	24 hours
No	Yes	Yes	High Priority Alert	7 hours	1 hour	24 hours
No	No	Yes	Low Priority Alert	24 hours	1 hour	48 hours

The service levels noted in the table above will become effective thirty (30) days following the Order Effective Date, to allow time for Customer to install Products and for FireEye to determine the level of staffing needed to respond to Alerts in Customer's environment.

(e) Extended Investigations; Multiple Related Alerts. When FireEye has identified a true positive or suspicious activity, FireEye analysts may perform an extended investigation, and/or may aggregate and review multiple Alerts from related Covered Systems to determine the extent of activity related to the Alert. FireEye analysts may append results from the extended investigation or subsequent Alert investigations to the initial FaaS Report if FireEye determines that additional or subsequent Alerts are related, and in such cases, FireEye will not be required to issue a separate FaaS Report for each such related Alert.

(f) Non-Remediable Alerts. FireEye has no obligation to notify the Customer or generate a new FaaS Report on new Alerts that are directly related to previous investigations where a FaaS Report has been published and FireEye has provided recommended remediation steps, when the Customer has acknowledged the FaaS Report but chooses not to or cannot remediate the cause of these Alerts.

(g) Alert Priority. FireEye may re-prioritize Alerts, regardless of their severity classification, to provide focus to Alerts that FireEye determines may have the largest impact to the Customer's environment.

(h) Continuity of Monitoring. All monitoring, investigation and reporting activities described in this Section 2.1 will be provided on a 24/7/365 basis.

2.2 System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, or FX Product, FireEye will provide Customer with notifications of system health issues such as connectivity problems.

2.3 Containment. When the Customer has purchased the HX Product, FireEye may, when appropriate, recommend containment of the target Covered System from the Customer's network. Containment must be executed by the Customer.

2.4 Portal Access. Alerts and FaaS Reports will be provided via an online portal ("FaaS Portal"), and FireEye will provide login credentials to the Customer to enable access to the FaaS Portal. The FaaS Portal will be available 99.9% of the time in any calendar month, other than Downtime, as defined below, and this FaaS Portal Service Level commitment will be subject to the Service Level Credits set forth in Section 3 below.

2.5 FireEye Intelligence Center. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

(a) Permitted Use; Reports. Customer may access, view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye IP. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

(b) Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100) queries of IP addresses and domain names and (B) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

(c) User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC, including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including CTI, to the extent such information is de-identified.

(d) Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

(e) Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

2.6 Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye authorized services or support partner (a "Partner"), Customer agrees that the Subscription and FaaS Reports may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription and Customer Data to Partner.

2.7 Customer Networks. The Subscription may only be provided for computer systems and networks leased to or owned by Customer, and under Customer's control, up to the number of Nodes allowed, as set forth in the applicable Subscription Order.

2.8 Connectivity Requirements. Unless otherwise specified, the Subscription are provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. Customer must provide outbound TCP-based connectivity from all Products to FireEye for the establishment of a virtual private network (VPN). Details pertaining to specific network access requirements will be established in conjunction with installation activities.

2.9 **Credential Security.** Customer will be responsible for the following: (a) providing accurate information to FireEye for provisioning access to (and removal of) Customer personnel access to the FaaS Portal; (b) implementing and adhering to strong password standards; (c) providing accurate information to FireEye for domain whitelisting; and (d) reporting any security issues related to the Subscription (including the FaaS Portal) to FireEye immediately.

2.10 **Exclusions.** Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence (DTI) Subscription; (iii)

Products with an installed FireEye operating system less than version 6.2; (iv) Products that have been declared end of life; (v) Products that have no active Support Service in place; (vi) Products for which software updates have not been applied; (vii) Products that have not been installed and deployed; or (viii) Products that are misconfigured or incorrectly deployed, which prevents the Products from monitoring the Covered Systems. Customer acknowledges that to facilitate FireEye's efficient performance of the Subscription, FireEye may control some features and functionality of the Products, and that such features or functionality may not be available for Customer's independent use during the Subscription Term.

3. FaaS Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the FaaS Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the FaaS Portal is not available due to a failure or a disruption in the FaaS Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the FaaS Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the FaaS Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the FaaS Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the FaaS Portal does not meet the monthly service availability defined in 3.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of FaaS Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences a disruption in availability of the FaaS Portal and ending when a successful solution or workaround allowing for full restoration of the FaaS Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the calendar month in which the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-2
SUBSCRIPTION TERMS FOR FIREEYE AS A SERVICE (FAAS) – CONTINUOUS VIGILANCE

The following terms govern the FireEye as a Service (FaaS) – Continuous Vigilance (CV) Subscription.

3 Definitions.

3.1 **"Alert"** means, individually and collectively, APT Alerts, High Priority Alerts, and Low Priority Alerts.

3.2 "**APT Alert**" means (a) with respect to Products other than HX, an alert generated by a Product, that is identified by the Product as being associated with a "targeted threat," which means advanced persistent threat (APT) actors or APT activity; (b) with respect to the HX Product, an alert designated by HX as XPLT, EXC, or PRE, that is triggered by a FireEye standard Indicator; and (c) with respect to the TAP Subscription, an "APT Alert" means a TAP Alert designated as an "APT Alert" in the table in Section 1.11 below.

3.3 "**APT Only Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of APT Alert. If Customer purchases the APT Only Service, FireEye will provide FaaS Reports and monitoring of only APT Alerts, and not any other Alerts.

3.4 "**Covered System**" means (i) a computing device (to the extent supported by FireEye) that Customer specifies as within the scope of the CV Subscription, and if the Customer has purchased the HX Product, on which a software agent has been installed to support CV Subscription delivery, or (ii) a computing device (to the extent supported by FireEye) whose network traffic is observable to support CV Subscription delivery; (iii) with respect to ETP Subscriptions, mailboxes monitored to support CV Subscription delivery; or (iv) any computing device that both Customer and FireEye agree is within scope of the CV Subscription.

3.5 "**Full Coverage Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of all Alerts, regardless of the severity level of the Alert as classified by the Product.

3.6 "**High Priority Alert Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of High Priority Alerts and APT Alerts.

3.7 "**FaaS Reports**" means the written reports relating to Alerts that FireEye creates and makes available to Customer through the CV Subscription.

3.8 "**High Priority Alert**" means (a) with respect to Products other than HX and FX, an alert generated by that Product that is classified by that Product as severity level "critical" or "major"; (b) with respect to the FX Product, any alert generated by the FX Product, including APT Alerts; and (c) with respect to a TAP subscription, a TAP Alert designated as a "High Priority Alert" in the table in Section 1.11 below.

3.9 "**Low Priority Alert**" means an alert generated by a Product or TAP Subscription (as applicable) that is not an APT Alert or a High Priority Alert.

3.10 "**Nodes**" or "**Node Band**" refers to number of Covered Systems within the Customer environment, which is reflected on the Subscription Order.

3.11 "**TAP Alert**" means an alert generated by the TAP Subscription, with a severity level assigned by the TAP Subscription (e.g., "Critical," "High," "Medium"). TAP Alerts are investigated and reported on as "APT Alerts" and "High Priority Alerts" as shown in the table below, depending on the TAP Rule Pack that invoked the TAP Alert:

FireEye Rule Pack	APT Alerts	High Priority Alerts
Application Detection		
Cloud Infrastructure		
Commodity Malware		All

Current Events	Critical, High	Critical, High
DTI Rules		All
Exploit Kits		All
FTP		
Industrial Control Systems	Critical, High, Medium	Critical, High, Medium
Intel Match	Critical, High, Medium	Critical, High, Medium
Linux		Critical, High
Malware Methodology		Critical, High
Phishing	Critical High	Critical, High
Point of Sale	All	All
Security Tools		Critical, High, Medium
Targeted Malware	All	All
Vendor – FireEye		
Vulnerability		Critical, High, Medium
Web Application Attacks		Critical, High, Medium
Windows		Critical, High

1.13 "**TAP Rule Packs**" means a predefined set of criteria that identifies suspicious events or threats based on the associated rule type within the TAP Subscription.

2 **Scope of FaaS – Continuous Vigilance (CV) Subscription**. During the Subscription Term, FireEye will provide the CV Subscription as set forth in this Section 2, according to the Subscription level purchased by Customer as set forth in the Subscription Order. If the Subscription Order does not specify the Subscription lvel purchased, then Customer will be deemed to have purchased the APT Only Service. All services Customer requests that are not described in this Section 2 will be performed at mutually agreed upon rates as set forth in Statements of Work. Unless otherwise specified, the CV Subscription is provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. The CV Subscription is available for the number of Nodes purchased (available for Customers who have purchased the FireEye NX, FX, or EX Product or the ETP or TAP Subscription). If the number of Nodes exceeds the amount reflected in the Subscription Order by more than ten percent (10%), FireEye will notify Customer in writing, and will issue an invoice for the next higher Node Band at FireEye's then-current rates pro-rated for the remaining portion of the then-current Subscription Term.

2.1 Event Analysis.

(e) Time to Begin Analysis. FireEye will begin analysis of an Alert within the times set forth in the table below, calculated from the time the Alert was generated by the Product or TAP Subscription (as applicable).

(f) Alerts Investigated. FireEye will investigate and report on the Alerts that correspond with the Subscription level the Customer purchased. If the Customer purchased the APT Only Service, FireEye will investigate and report on only APT Alerts. If the Customer purchased the High Priority Alerts Service, FireEye will investigate and report on only High Priority Alerts and APT Alerts. If the Customer purchased the All Alerts Service, FireEye will investigate and report on APT Alerts, High Priority Alerts, and Low Priority Alerts. FireEye has no obligation to investigate and report on Alerts that fall outside the purchased Subscription level.

(g) Initial Investigation. FireEye analysts will perform an initial analysis of the Customer's Covered Systems to determine if the Alert is a true or false positive, benign or suspicious activity.

(h) FaaS Reports. If FireEye's investigation determines that the Alert indicates a true compromise, FireEye will publish a FaaS Report to the FaaS Portal within one (1) hour of the time FireEye makes that determination. Regardless of whether FireEye's investigation determines that an Alert indicates a true compromise, FireEye will publish a FaaS Report on the Alert to the FaaS Portal within the times set forth in the table

below, based on the classification of the Alert (APT Alert, High Priority Alert, Low Priority Alert). Customer acknowledges that in some cases, when FireEye's investigation is not complete, a FaaS Report may provide only an update of current status of the Alert investigation.

Alerts Investigated (Level of Service)			**FaaS Alert Classification**	**Time to Begin Investigation (from time Product or TAP Subscription generates Alert)**	**Time to Publish FaaS Report (from time FireEye validates actual compromise)**	**Time to Publish FaaS Report (when no validation of actual compromise; from time Product or TAP Subscription generates Alert)**
APT Only Service	**High Priority Alerts Service**	**Full Coverage Service**				
Yes	Yes	Yes	APT Alert	1 hours	1 hour	24 hours
No	Yes	Yes	High Priority Alert	7 hours	1 hour	24 hours
No	No	Yes	Low Priority Alert	24 hours	1 hour	48 hours

The service levels noted in the table above will become effective thirty (30) days following the Order Effective Date, to allow time for Customer to install Products and for FireEye to determine the level of staffing needed to respond to Alerts in Customer's environment.

(e) Extended Investigations; Multiple Related Alerts. When FireEye has identified a true positive or suspicious activity, FireEye analysts may perform an extended investigation, and/or may aggregate and review multiple Alerts from related Covered Systems to determine the extent of activity related to the Alert. FireEye analysts may append results from the extended investigation or subsequent Alert investigations to the initial FaaS Report if FireEye determines that additional or subsequent Alerts are related, and in such cases, FireEye will not be required to issue a separate FaaS Report for each such related Alert.

(f) Non-Remediable Alerts. FireEye has no obligation to notify the Customer or generate a new FaaS Report on new Alerts that are directly related to previous investigations where a FaaS Report has been published and FireEye has provided recommended remediation steps, when the Customer has acknowledged the FaaS Report but chooses not to or cannot remediate the cause of these Alerts.

(g) Alert Priority. FireEye may re-prioritize Alerts, regardless of their severity classification, to provide focus to Alerts that FireEye determines may have the largest impact to the Customer's environment.

(h) Hunting. FireEye will conduct periodic proactive hunting techniques on Covered Systems to look for additional indicators of malicious or attacker activity. When FireEye's investigation reveals a compromise, then within one (1) hour of the time FireEye makes that determination, FireEye will publish a FaaS Report related to that activity to the FaaS Portal.

(i) Continuity of Monitoring. All monitoring, investigation and reporting activities described in this Section 2.1 will be provided on a 24/7/365 basis.

2.2 System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, or FX Product, FireEye will provide Customer with notifications of system health issues such as connectivity problems.

2.3 Containment. When the Customer has purchased the HX Product, FireEye may, when appropriate, recommend containment of the target Covered System from the Customer's network. Containment must be executed by the Customer.

2.4 Portal Access. Alerts and FaaS Reports will be provided via an online portal ("FaaS Portal"), and FireEye will provide login credentials to the Customer to enable access to the FaaS Portal. The FaaS Portal will be

available 99.9% of the time in any calendar month, other than Downtime, as defined below, and this FaaS Portal Service Level commitment will be subject to the Service Level Credits set forth in Section 3 below.

2.5 FireEye Intelligence Center. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

(f) Permitted Use; Reports. Customer may access, view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye IP. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

(g) Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100) queries of IP addresses and domain names and (B) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

(h) User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC, including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including CTI, to the extent such information is de-identified.

(i) Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

(j) Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

2.6 Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye authorized services or support partner (a "Partner"), Customer agrees that the Subscription and FaaS Reports may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription and Customer Data to Partner.

2.7 Customer Networks. The Subscription may only be provided for computer systems and networks leased to or owned by Customer, and under Customer's control, up to the number of Nodes allowed, as set forth in the applicable Subscription Order.

2.8 Connectivity Requirements. Unless otherwise specified, the Subscription are provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. Customer must provide outbound TCV-based connectivity from all Products to FireEye for the establishment of a virtual private network (VPN). Details pertaining to specific network access requirements will be established in conjunction with installation activities.

2.9 **Credential Security.** Customer will be responsible for the following: (a) providing accurate information to FireEye for provisioning access to (and removal of) Customer personnel access to the FaaS Portal; (b) implementing and adhering to strong password standards; (c) providing accurate information to FireEye for domain whitelisting; and (d) reporting any security issues related to the Subscription (including the FaaS Portal) to FireEye immediately.

2.10 **Exclusions.** Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence (DTI) Subscription; (iii) Products with an installed FireEye operating system less than version 6.2; (iv) Products that have been declared end of life; (v) Products that have no active Support Service in place; (vi) Products for which software updates have not been applied; (vii) Products that have not been installed and deployed; or (viii) Products that are misconfigured or incorrectly deployed, which prevents the Products from monitoring the Covered Systems. Customer acknowledges that to facilitate FireEye's efficient performance of the Subscription, FireEye may control some features and functionality of the Products, and that such features or functionality may not be available for Customer's independent use during the Subscription Term.

3. FaaS Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the FaaS Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the FaaS Portal is not available due to a failure or a disruption in the FaaS Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the FaaS Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the FaaS Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the FaaS Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the FaaS Portal does not meet the monthly service availability defined in 3.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of FaaS Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences a disruption in availability of the FaaS Portal and ending when a successful solution or workaround allowing for full restoration of the FaaS Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the calendar month in which the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-3
SUBSCRIPTION TERMS FOR FIREEYE THREAT ANALYTICS PLATFORM (TAP)

The following terms govern the Threat Analytics Platform Subscription, including purchase and support of TAP Cloud Collector™ Appliances and Support.

1. TAP Software, Alerts

1.1.1 TAP Software and Hardware. As part of the TAP Subscription, FireEye may deliver to Customer one or more software files (individually and collectively, "TAP Software"), and/or one or more "Cloud Collector" hardware appliances ("Cloud Collector Appliances"), which may contain TAP Software. Subject to full payment of all Fees associated with the TAP Subscription, FireEye grants to Customer a non-exclusive, limited right and license to install and run the TAP Software during the Subscription Term solely for purposes of using the TAP Subscription in accordance with the Documentation for the TAP Subscription.

1.1.2 Access; Customer Logs. FireEye will provide Customer with credentials to enable access to the TAP Subscription. Using the TAP Software, and subject to payment of Fees for the TAP Subscription and any Cloud Collector Appliances, Customer may upload Customer Logs to the TAP portal ("TAP Portal"). "Customer Logs" means any communications, logs and other content and information that Customer or anyone using Customer's account contributes to or through the TAP Portal. Customer grants to FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive license and right to reproduce, modify, create derivative works from, publish, distribute, sell, sub-license, transmit, publicly display and provide access to Customer Logs, for purposes of enhancing FireEye's products and services, so long as (i) FireEye ensures that any Customer Confidential Information is removed from Customer Logs, and (ii) FireEye's use of Customer Logs does not in any way identify Customer or its employees or in any other way allow a third party to identify Customer as the source of the Customer Logs. Customer Logs are Customer's property, and other than the licenses granted in herein, FireEye does not obtain any ownership rights in Customer Logs.

1.1.3 TAP Alerts. Some features of the TAP Subscription may generate alerts of suspected malicious activity (each, a "TAP Alert"). TAP Alerts are FireEye Materials. FireEye hereby grants to Customer a limited, non-exclusive right to use TAP Alerts, and reproduce and distribute those TAP Alerts internally for Customer's own business purposes.

1.1.4 Cloud Collector Management. If Customer has installed Cloud Collectors in connection with the TAP Subscription, then FireEye will continuously monitor the Customer's Cloud Collector Appliances or Cloud Collector TAP Software for system health issues such as monitoring to ensure proper throughput and relay of data.

1.1.5 Cloud Collector Appliances. If the Customer has purchased Cloud Collector Appliances, then during the TAP Subscription Term, FireEye will replace any defective Cloud Collector Appliances as follows:

a) Prior to any return, Customer shall verify that the Cloud Collector Appliance at issue is defective by logging a Support request via one of the mechanisms provided in the Documentation and in accordance with FireEye's RMA procedures, including providing the part number, serial number, quantity and reason for return, an explanation of all failure symptoms and other relevant information.

b) Upon confirmation by FireEye of a defect, Customer shall obtain from FireEye an RMA number. FireEye shall ship via a recognized express courier service a replacement Cloud Collector Appliance to Customer to arrive no later than next business day after FireEye's issuance of an RMA number, provided the RMA number was issued prior to the business day cutoff time local to the defective Cloud Collector Appliance, provided the replacement does not require any custom pre-configuration, and provided no external-to-FireEye circumstances prevent the delivery. The replacement Cloud Collector Appliance may be a new or reconditioned Cloud Collector Appliance (of equivalent or better quality) at FireEye's sole discretion.

c) FireEye shall pay the shipping costs to ship the replacement Cloud Collector Appliance to Customer, but Customer shall bear any and all risk of loss of or damage to said Cloud Collector Appliance at all times after said Cloud Collector Appliance is made available by FireEye to the common carrier.

d) Within five (5) business days after Customer receives the replacement Cloud Collector Appliance from FireEye, Customer shall package the defective Cloud Collector Appliance in its original packing material or equivalent, write the RMA number on the outside of the package and return the defective Cloud Collector Appliance, at FireEye's cost (provided Customer utilizes FireEye's designated courier service and properly packages the defective Cloud Collector Appliance according to FireEye's instructions), shipped properly insured, FOB FireEye's designated facility. Customer shall enclose with the returned Cloud Collector Appliance the applicable RMA form, and any other documentation or information requested by FireEye customer support. Customer shall assume any and all risk of loss of or damage to such Cloud Collector Appliance during shipping. Title to the defective Cloud Collector Appliance shall pass to FireEye upon FireEye's receipt thereof.

e) When a replacement Cloud Collector Appliance is provided and Customer fails to return the defective Cloud Collector Appliance to FireEye within ten (10) business days after Customer receives the replacement Cloud Collector Appliance from FireEye, FireEye may charge Customer, and Customer shall pay for the replacement Cloud Collector Appliance at the then-current list price.

2. Event Volume; True-Up

2.1.1 Fees for the TAP Subscription are divided into "Tiers" based on the volume of events processed through the TAP Subscription per second ("Event Volume"). If at any point during the Subscription Term, Customer's Event Volume exceeds the Tier upon which Customer's TAP Subscription Fees were based, FireEye will not guarantee that Customer Logs in excess of the purchased Tier will be ingested and processed by the TAP Subscription. In times of Event Volume in excess of the paid Tier, Customer Logs will enter a queue. Excessive queueing may cause Customer Logs to be lost from the queue. If at any point during the Subscription Term, Customer's average Event Volume for any consecutive thirty-day period exceeds the Tier upon which Customer's TAP Subscription Fees were based, FireEye may issue a true-up invoice for the pro-rated difference between the Fees already paid for that Subscription Term and FireEye's list prices for the Fees for the Tier associated with Customer's actual Event Volume for that thirty-day period, pro-rated to reflect that thirty-day period and the remainder of the Subscription Term. FireEye will apply any discounts that were applied to initial Fees to FireEye's list prices for any true-up invoice. Until such time that the True Up invoice is paid in full, the TAP Subscription will continue to ingest and process only the Event Volume of the purchased Tier, allowing any excess Customer Logs to enter queueing conditions. The Tier for any Renewal Subscription Term will be the Tier associated with the actual Event Volume for the immediately preceding Subscription Term.

2.1.2 At the end of the Initial Subscription Term and each Renewal Subscription Term, FireEye may true-up Fees for that Subscription Term, and if the average monthly Event Volume for that Subscription Term exceeds the maximum Event Volume for the Tier for which Customer previously paid Fees, then (a) FireEye will issue a true-up invoice reflecting the difference between the Fees already paid for that Subscription Term and the Fees for the Tier associated with Customer's actual Event Volume.

3. TAP Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the TAP Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the TAP Portal is not available due to a failure or a disruption in TAP Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the TAP Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the TAP Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the TAP Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the TAP Portal does not meet the monthly service availability defined in 6.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of TAP Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences unavailability of the TAP Portal and ending when a successful solution or workaround allowing for full restoration of the TAP Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the date the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

4. FireEye Intelligence Center™ (FIC™), Community Threat Intelligence™ (CTI™). During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

i. Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

ii. Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100)queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

iii. User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform, to the extent such information is de-identified.

iv. Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

v. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-4
SUBSCRIPTION TERMS FOR FIREEYE EMAIL THREAT PREVENTION (ETP) and MOBILE THREAT PREVENTION (MTP)

The following terms govern the Email Threat Prevention Subscription and Mobile Threat Prevention Subscription.

1. Definitions.

"Cloud Subscription" means the online, web-based applications and platform which is made accessible to Customer by FireEye via a designated website, which includes the associated offline Software components to be used in connection with FireEye Mobile Threat Prevention and/or FireEye Email Threat Prevention. FireEye Mobile Threat Prevention ("MTP") and FireEye Email Threat Prevention ("ETP") are separate Cloud Subscriptions and usage is conditional on what the Customer has indicated on an Order.

"Customer Data" means data, information, applications, and any other items originated by Customer that Customer submits to the Cloud Subscription.

"Customer Representatives" means any employee or contractor of Customer or Mobile Device Manager to whom Customer provides access to the Cloud Subscriptions (or any component thereof, including Software) for use on behalf of and for the benefit of the Customer and for Customer's internal business purposes, subject to all the terms and conditions of this Agreement.

"Licensed Device" means (i) with respect to MTP, the registered devices that Customer may have at any time that are registered to the Cloud Subscription; which maximum number shall be based on the subscription fees paid by Customer and identified on the relevant purchase order from Customer as approved and invoiced by FireEye; and (ii) with respect to ETP, the number of email inboxes Customer may have at any time that are registered to the Cloud Subscription; which maximum number shall be based on the subscription fees paid by Customer and identified on the relevant purchase order from Customer as approved and invoiced by FireEye. For the avoidance of doubt, with respect to MTP, "registered devices" are those devices which have loaded device Software and which have been registered to the Cloud Subscription and which have not been retired (meaning unregistered).

"Mobile Device Manager" shall mean a third party who has been engaged by the Customer to provide security services for Licensed Devices for the benefit of Customer. Where indicated as such, the Mobile Device Manager shall be a subset of the definition of the Customer Representatives solely as applicable to MTP.

"Software" means the object code version of FireEye's proprietary computer programs delivered to Customer hereunder for use in connection with the Cloud Subscriptions, including collectively and individually the device-side software used on devices registered to the Cloud Subscription ("Device Software") and any connector software and/or any other server-side software (collectively the "Premise Software") , each which are delivered to Customer hereunder for use in connection with the Cloud Subscriptions, and any Documentation, backup copies and updates, upgrades, maintenance releases, bug fixes to any of the forgoing provided to Customer hereunder.

2. Right of Access and Use. During the Subscription Term, and subject to the terms of this Agreement, FireEye grants to Customer a non-exclusive right to (a) permit those Customer Representatives authorized by Customer to access and use the Cloud Subscriptions on Customer's behalf in compliance with the terms of this Agreement, and (b) to install, copy and use Premise Software in connection with Cloud Subscriptions in accordance with the Agreement and this Exhibit, but solely on systems and hardware owned or controlled or otherwise managed by Customer on behalf of and for the benefit of Customer, (c) to install, copy and use Device Software in connection with Cloud Subscriptions in accordance with the Documentation, but solely on devices used by Customer Representatives on behalf of and for the benefit of Customer. Notwithstanding anything else herein, the number of devices Customer and/or Customer Representatives may register to the Cloud Subscriptions may not exceed the number of Licensed Devices.

Notwithstanding anything to the contrary herein, if Customer is using the Cloud Subscriptions for evaluation purposes then such Customer usage is solely for internal testing and evaluation and the Subscription Term shall not exceed fifteen (15) days unless otherwise mutually agreed upon in a signed Evaluation License Agreement.

3. Restrictions. Except as otherwise expressly permitted under this Agreement, Customer agrees that it shall not, nor shall it permit any third party to, (a) use the Cloud Subscriptions (or any portion thereof) in excess of or beyond the Subscription Term, the Licensed Device quantity, and/or other restrictions/limitations described in this Agreement; use the Cloud Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or other rights; (d) interfere with or disrupt the integrity or performance of the Cloud Subscriptions or third-party data contained therein; (e) use the Software on equipment or devices which are not specified in the Documentation; (f) Cloud Subscription specific to ETP Cloud Subscriptions, Customer shall route email through a commercially available secure email gateway for anti-spam scanning prior to relay through the FireEye network. No rights or licenses are granted other than as expressly and unambiguously set forth herein. Customer access and usage for the Cloud Subscriptions is limited to the MTP or ETP Subscription that has been paid or are being evaluated by the Customer.

4. Updates, Malware Detection Content and Support Services. Updates and malware detection content and/or support services are not necessarily provided with the Software or Subscriptions, and may require additional payment or include additional terms and conditions. However, to the extent that an update to the Software and/or malware detection content is provided, such update/content shall be deemed "Software" provided subject to this Agreement. If malware detection content/support services are provided, FireEye reserves the right to change the scope or duration of such services at anytime, and to access, freely use and distribute data collected from Customer through such services. If such services are made available, Customer may be required to pay fees or other charges for use or access to some or all such services, which fees and terms will be specified in the invoice or order form for such service.

5. Device Count Increases; Reporting; Invoice. If the number of devices that Customer or Customer Representatives have registered to the Cloud Subscription ("Actual Device Count") exceeds Customer's then current Licensed Device count or if Customer wishes to increase the Licensed Device count, then Customer shall notify FireEye (or the applicable FireEye Partner) and submit an Order for the incremental Subscription Fees due, and upon receipt of such Order, the Licensed Device count shall be amended to reflect this change. Upon written request, Customer will provide FireEye a report identifying (i) the Actual Devices; (ii) the copies of and location of the Premise Software maintained; and (iii) any other information reasonably requested by FireEye at the time as it relates to the use of the Cloud Subscription to determine compliance with the terms of this Agreement. FireEye and/or its Authorized Resellers may invoice Customer if it learns of any shortfalls, i.e. that the Licensed Device Count is below the Actual Device count. The fees charged to Customer for increases in License Device counts will be based on the then-current Subscription Term pricing.

6. Cloud Subscription Availability

6.1 FireEye shall undertake commercially reasonable efforts to ensure the Cloud Subscription availability for 99.9% of the time during each calendar month.

6.1.1 "Service Outage" is where the Customer is not receiving Cloud Subscription due to a failure or a disruption in the Cloud Subscriptions and is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

6.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the Cloud Subscriptions may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

6.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the Cloud Subscriptions during the Emergency Maintenance.

6.1.4 "System Availability" means the percentage of total time during which the Cloud Subscriptions shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

6.2. Remedy

6.2.1 In the event that the Cloud Subscription does not meet the monthly service availability defined in 6.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of System Availability per Calendar Month	Service Credit
<99.9%	25%
<99.0%	50%
<98.0%	100%

6.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when there is a disruption in Cloud Subscription and ending when a successful solution or workaround allowing for full restoration of the Cloud Subscriptions is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the date the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

6.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

6.2.4 Customer shall not be entitled to receive a Credit that exceeds 100% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-5
SUBSCRIPTION TERMS FOR FIREEYE ADVANCED THREAT INTELLIGENCE PLUS (ATI+)

The following terms govern the Advanced Threat Intelligence Plus (ATI+) Subscription.

The ATI+ Subscription comprises two features: Continuous Monitoring ("CM" or "Continuous Monitoring") and the FireEye Intelligence Center™ (FIC™) ("FIC").

1. Continuous Monitoring

The Continuous Monitoring portion of the Subscription is purchased in connection with one or more FireEye Products, and includes the following during the Subscription Term for the specific Products for which Continuous Monitoring was purchased (some Products may not be eligible for CM):

(a) Critical Event Notification. For Customers who have purchased the FireEye NX, FX, HX or EX Product, MVX Smart Grid with Network Smart node product combination, or the ETP or TAP Subscription, FireEye will provide Customer with proactive notifications of events FireEye determines to be critical that are logged by the Products ("Alerts"). FireEye will also provide Customer with access to a detailed description of the Alert. Alerts are not proof of vulnerability, threats or attacks on Customer.

(b) System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, FX, HX AX or FX Product, or MVX Smart Grid w/Network Smart node combination (hardware only), FireEye will provide Customer with proactive notifications of serious system health issues related to the hardware for Products covered by Continuous Monitoring. Customers will also be provided with metrics on critical event notifications and, for purchased hardware, the status of monitored hardware parameters.

(c) Portal Access. Alerts and critical event notifications from Continuous Monitoring will be provided via an online portal, and FireEye will provide login credentials to the Customer to enable access to that portal.

(d) Continuity of Monitoring. The monitoring activities described in (a)-(c) above will be provided on a 24/7 basis.

(f) Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye Partner, Customer agrees that the Subscription may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription to the Partner.

(g) Exclusions. Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence subscription; (iii) Products with an installed FireEye operating system less than version 6.2; (iv) Products that are end of life; (v) Products that have no active support service in place; (vi) Products for which software updates have not been applied; or (vii) Products that have not been installed and deployed.

2. FireEye Intelligence Center™ (FIC™), Community Threat Intelligence™ (CTI™)

FireEye will provide the FIC portion of the Subscription, which includes the Community Threat Intelligence (CTI) platform, during the Subscription Term, as set forth below:

2.1 Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

2.2 Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (i) one hundred (100) queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware per day. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

2.3 User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform. Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform to the extent such information is de-identified.

2.4 Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-6
SUBSCRIPTION TERMS FOR FIREEYE INTELLIGENCE CENTER™ (FIC™) (INCLUDING COMMUNITY THREAT INTELLIGENCE™ (CTI™))

The following terms govern the FireEye Intelligence Center™ (FIC™) Subscription, which includes access to the Community Threat Intelligence™ (CTI™) platform.

1. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

i. Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

ii. Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100)queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

iii. User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform, to the extent such information is de-identified.

iv. Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

v. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-7
SUBSCRIPTION TERMS FOR FIREEYE iSIGHT INTELLIGENCE

The following terms govern the FireEye iSIGHT Intelligence Subscription ("iSIGHT" or "iSIGHT Subscription"). FireEye will provide the iSIGHT Subscription purchased by the Customer, as shown on the Order.

1. Definitions.

1.1 "Access Method(s)" or "Access Methods" means the MySIGHT Portal ("MySIGHT"), Software Development Kit ("SDK"), Application Programming Interface ("API"), Browser Plugin, iSIGHT App for Splunk, or any other method provided by FireEye for Customer to access the iSIGHT Subscription, individually or collectively. All Access Methods are FireEye Material as defined in the Agreement.

1.2 "Application" is a software program the Customer creates, or causes to have created on its behalf, that is designed to access the Content, which includes the features of the SDK/API but adds significant functionality beyond that provided by the SDK/API.

1.3 "Application Programming Interface" or "API" means the latest version of the iSIGHT Application Programming Interface software made generally available by iSIGHT, with its developer's guide and other related material (available at http://www.isightpartners.com).

1.4 "Browser Plugin" means the iSIGHT Browser Plugin which a Customer may install on Google Chrome and/or other commercially available and supported browsers that allows the Customer to access and view the Content when licensed to do so. The Browser Plugin displays the iSIGHT logo and links to MySIGHT. The Browser Plugin includes the latest version of the Browser Plugin software, its documentation and any html embedded code.

1.5 "Content" means the cyber threat intelligence data and any reports, threat indicators, trends, events, information, documentation or functionality provided in connection with the iSIGHT Subscription. All Content is FireEye Material as defined in the Agreement.

1.6 "End User" means the Customer or the Customer's employees, as applicable.

1.7 "Software Development Kit" or "SDK" shall mean the latest publicly-available version of the iSIGHT Software Development Kit and any associated documentation, tools, libraries, technical notes, software code, or other materials.

1.8 "iSIGHT App for Splunk" means the application provided by FireEye, which a Customer may install on Splunk, that allows the Customer to access and view the Content in accordance with this Agreement. The iSIGHT App for Splunk includes the latest version of the iSIGHT App for Splunk software, its documentation and any html embedded code.

1.9 "iSIGHT Subscription" includes but is not limited to, Cyber Crime, Cyber Espionage, Critical Infrastructure, Enterprise, Hacktivism, Vulnerability and Exploitation, MySIGHT Portal, Global Response, Analyst Access, iSIGHT SDK, iSIGHT API, iSIGHT Research Reports, or the current offering(s) as listed on the iSIGHT website, and as purchased by the Customer as shown on the Order.

2. License; Access to iSIGHT Subscription and Content.

2.1. Grant of Limited License. During the Subscription Term, FireEye grants to Customer in strict accordance with the terms of this Agreement, a limited, worldwide, revocable, non-exclusive, non-transferable, non-assignable, non-sublicensable royalty-free right and license to:

(a) use MySIGHT, the iSIGHT Subscription, and any Content provided by FireEye for internal use only. The ISIGHT Subscription can be used by End Users who have a valid "need to know" within Customer's organization, typically defined as a person or group that has a direct role in securing information system or networks. FireEye agrees to provide support for the ISIGHT Subscription in accordance with Section 3 below ("Subscription Support" or "Support").

(b) use the API to search, display, and otherwise access the Content. The API can be used to develop, display, or integrate applications, scripts, tools or workflows that interoperate with iSIGHT Subscriptions for the Customer's internal use. FireEye agrees to provide Support for the latest version of the API in accordance with Section 3 below.

(c) download, install and use the Software Development Kit ("SDK") to design, develop and test an Application(s), for the Customer's internal use only, for the purpose of customizing access to the Content. The Customer may modify the source code versions of sample files, if any, included with the SDK for the purpose of creating Customer's Application(s), and may make a reasonable number of copies of the SDK as necessary to develop Customer's Application(s), provided that Customer must reproduce complete copies of the SDK, including without limitation all "read me" files, copyright notices, and other legal notices and terms. FireEye agrees to provide Support for the ISIGHT SDK in accordance with Section 3 below.

(d) use the Browser Plugin to search, display and otherwise access the Content for the Customer's internal use only. Customer may install and use one copy of the Browser Plugin on a single computer per license. FireEye agrees to provide Support for the latest version of the Browser Plugin in accordance with Section 3 below

(e) use the ISIGHT App for Splunk to search, display and otherwise access the Content for the Customer's internal use only. Customer may install and use one copy of the ISIGHT App for Splunk on a single computer per license. FireEye agrees to provide Support for the latest version of the ISIGHT App for Splunk in accordance with Section 3 below.

2.2. Access Keys. Use of the Access Methods and access to the ISIGHT Subscription and the Content by Customer's End Users is provided through access keys or login credentials. Access keys in association with the Access Methods and ISIGHT Subscription shall be kept in confidence by Customer and Customer's End Users. Access keys will be issued to individual End Users by FireEye in accordance with each particular Access Method's parameters and will not be shared between End Users. Customer may not establish group accounts. Any unauthorized disclosure or dissemination of access keys by Customer or End Users shall be deemed a material breach of this Agreement. Customer shall inform FireEye of any data breach concerning login credentials in a timely manner. FireEye reserves the right to change, suspend, remove, or disable Customer's access keys to the Access Methods, ISIGHT Subscription , and Content upon notice if a material breach is suspected and not rectified upon notification.

2.3. Latest Version. The license granted to Customer under this Agreement is for the current version of the Access Methods. FireEye may release future versions of the Access Methods as determined in the sole discretion of FireEye. Nothing in this Agreement is a commitment to Customer of compatibility between the existing Access Methods and any future versions of the Access Methods. FireEye reserves the right to discontinue offering particular Access Methods (or any updates thereto) or to modify the Access Methods at any time in its sole discretion.

2.4. Multiple Copies. Customer may receive software for an Access Method in more than one medium and/or in multiple copies. The Customer's license rights are in accordance with the Order regardless of the number of copies received.

2.5. Additional Licenses. Customer may purchase additional licenses for the Browser Plugin for its authorized End Users through the Chrome Web Store. Customer may purchase additional licenses for the ISIGHT App for Splunk for its authorized End Users through Splunk. Additional licenses for the Browser Plugin and ISIGHT App for Splunk may be purchased and will be valid for the current Subscription Term as provided in the Order.

2.6. Customer Application. The Customer may allow Customer's employees to access and use the SDK/API on Customer's behalf to design an Application. The Customer may not rent, lease, sell, transfer, sublicense or time-share the Customer's Application to any third-party without the express consent of FireEye. Customer shall retain all right, title or interest in the Application and as such, Customer agrees to indemnify and hold harmless FireEye for any claims of infringement made against FireEye in connection with any Application. The Customer's Application(s) must perform in accordance with the terms of this Agreement and must ensure the security and confidentiality of FireEye's Confidential Information. Customer assumes full responsibility for any breach of

security caused by Customer's Application(s) in connection with the Content, API, SDK, and specifically to any unauthorized disclosure of any FireEye Materials or FireEye Confidential Information.

2.7. Content Modifications. Customer may access the Content from the MySIGHT Portal, via email, SMS, HTML, API, any other Access Methods as officially distributed by FireEye or an FireEye sanctioned third-party integration. FireEye reserves the right to modify, amend, augment, reduce or alter the Content's format, or Access Methods, or mode of retrieval of the Content, that in the sole judgment of FireEye is in its customers' best interests. Customer will be entitled to retrieve the Content with any updates, modifications, additions or changes in the Content. These changes may require Customer to upgrade its systems, hardware or software and FireEye will not be responsible for the costs of any such changes.

2.8. Prohibited Usage. Customer must comply with any Intellectual Property rights asserted in any materials contained in the Content. The following conduct and usage restrictions apply during Customer's download, installation, and use of the Content and/or Access Methods, and survive termination of the Agreement or Subscription Term. Customer and its authorized End Users may not:

a. rent, lease, lend, sell, redistribute or sublicense any part of the ISIGHT Subscription or Access Methods to any other party;

b. share the ISIGHT Subscription , Access Methods, Content or Confidential Information with any third-parties, except as expressly authorized in advance by this Agreement or by FireEye in writing;

c. use the ISIGHT Subscription or Access Methods in the operation of a service or in any way to provide services to any third-party;

d. create derivative works for external distribution or use based upon the Content;

e. create apps, extensions, or other products and services that use Content except as set forth herein;

f. display, post, frame, or scrape the Content, except as allowed under this Agreement;

g. use the Access Methods for any other purpose than to access the ISIGHT Subscription and the Content;

h. use the Access Methods for any illegal or unauthorized purpose to promote or provide instructional information about illegal activities or to promote stalking, physical harm or injury against any group or individual, or any use that violates the rights of privacy and publicity of others;

i. create, place, or disseminate any materials or other items that are inappropriate, defamatory, obscene, pornographic, harassing, threatening, abusive, hateful or otherwise offensive, or is unlawful (including any content that infringes any patent, trademark, service mark, copyright, trade secret or other proprietary right of any third-party without appropriate permissions);

j. transmit any viruses, worms, defects, Trojan horses, time-bombs, malware, spyware, or any other computer code of a destructive or interruptive nature in connection with use of the Access Methods;

k. use the Access Methods in connection with or to promote any products, services, or materials that constitute, promote or are used primarily for the purpose of dealing in spyware, adware, or other malicious programs or code, counterfeit goods, unsolicited mass distribution of email ("spam"), hacking, surveillance, interception, descrambling equipment, stolen products and items used for theft;

l. create any Application that exposes or provides functionality of the Access Methods to any third party;

m. interfere, restrict or inhibit any other customer from using the Access Methods or Content or disrupt any services offered by FireEye through any medium;

n. attempt to exceed or exceed the usage limits established by FireEye for the Customer (http://www.isightpartners.com/doc/sdk-bp-docs/#/rate_limiting).

2.9. Restrictions. FireEye expressly reserves the right to limit the number and/or frequency of requests for Content made through the Access Methods in its sole discretion in line with technical design and performance standards as documented in the publicly available developers guide. FireEye may limit the number of network calls that any Application may make via the Access Methods, the maximum file size, or the maximum amount of ISIGHT material that may be accessed. FireEye may change such usage limitations at any time and without notice. In addition to any other rights under this Agreement, FireEye may utilize technical measures to prevent over-usage or to stop usage of any Access Methods or any Application after any usage limitations are exceeded. The most current API/SDK documentation and developers guide can be found at http://www.isightpartners.com/doc/sdk-bp-docs/#/, and these documents detail the current rates and capabilities of the API.

2.10. Customer recognizes and agrees that certain information and data that will be provided by Customer to FireEye pursuant to the ISIGHT Subscription is not owned by Customer and is not Confidential Information of

Customer. Malware submitted by Customer to FireEye for analysis under ISIGHT Global Response, and other information submitted by Customer to FireEye that is not unique to and/or developed by Customer (collectively "Submissions") shall not be considered Confidential Information or Intellectual Property of the Customer. FireEye may use the Submissions, aggregate the Submissions with submissions from other FireEye customers as well as original research and analysis, and share that aggregated intelligence with Customer and with other FireEye customers to enhance the services FireEye provides to its customers. FireEye will anonymize all Submissions prior to distribution, and will not identify the source of any Submission without written permission in each case.

3. Service Levels.

3.1. Service Call and Subscription Support

FireEye maintains a service desk in order to assist its customers with issues, trouble or general questions concerning use of the FireEye ISIGHT Products. Customer may initiate a service call as follows:

Description	Details
FireEye Service Desk (Primary, escalation and off-hours contact)	servicedesk@isightpartners.com
Service Desk Hours	24 x 7
Service Call Response Time ("Response Time Standard")	4 hours for initial response (confirmation of receipt is immediate through an automated ticketing system)
ISIGHT API	General information regarding ISIGHT API which can be accessed at http://www.isightpartners.com/doc/api2.0/docs/#/
Other resources (all other Subscription Support issues)	Existing Clients – Contact your assigned Intelligent Account Manager at: client-engagement@isightpartners.com Prospective Clients – Contact your assigned Sales Engineer at: sales-engineering@isightpartnerns.com Partners, Resellers, Referrals – Contact partners program representative at: partners@isightpartners.com

FireEye will catalog and evaluate all bugs or software issues as they are reported. Such issues will be prioritized based on variables such as customer impact, security impact, etc. and will be scheduled for release accordingly. When applicable, FireEye will notify Customer of urgent patches or bug fixes. Support Services do not include custom programming services, on-site support, or other services including installation of hardware or software, or training.

3.2. Maintenance and Updates

(a) When feasible and appropriate, FireEye will provide Customer prior notification about major releases at least two weeks in advance via communication from FireEye representatives.
(b) Scheduled system maintenance will be performed during the targeted times of 01:00 – 07:00 UTC on Thursdays and 12:00 – 19:00 UTC on Sundays. Prior notification will be provided in the event of any impact to customer facing applications.
(c) Emergency maintenance notifications will be provided by FireEye as early as possible but with a goal of six (6) hours' prior notice provided. Further, FireEye will strive to minimize the impact of any maintenance on any critical system during standard business hours around the globe.

3.3. Subscription Availability

(a) The FireEye ISIGHT API will have at least 99% system uptime ("API Uptime Standard").

(b) The iSIGHT MySIGHT Portal will have at least a 99% system uptime ("Portal Uptime Standard").

(c) FireEye realizes that a failure to meet the Response Time Standard, API Uptime Standard and the Portal Uptime Standard (collectively, the "Service Level Standards") could have an adverse impact to Customer. If FireEye fails to meet any of the Service Level Standards ("Service Level Failure"), FireEye will: (i) promptly investigate and report on the root cause of the problem; (ii) advise Customer of the remedial efforts being undertaken with respect to this failure to meet the Service Level Standards; (iii) use commercially reasonable efforts to correct the problem and begin meeting the Service Level Standards; and (iv) take appropriate preventative measures designed to ensure that the problem does not recur.

EXHIBIT C
FIREEYE SUPPORT SERVICES APPLICABLE FOR FIREEYE PRODUCTS

1. SUPPORT PURCHASED SEPARATELY FROM THE PRODUCTS. In the event Customer has purchased the Products and pass-through Support Services from FireEye through a FireEye authorized reseller (a "Reseller"), Customer will be entitled to all the rights herein set forth related to the level of Support Service requested and paid for by it, provided Customer: (a) is the original purchaser of the covered Products, (b) has provided true, accurate, current and complete information to FireEye included with its purchase; and (c) has maintained and updated this information to keep it true, accurate, current, and complete.

2. SUPPORT SERVICES PROVIDED BY FIREEYE.

FireEye offers a range of programs for the support of its Products as described below ("Support Programs"). Customer shall be entitled to receive the Support Services specified on the applicable support invoice and described below to the extent that Customer has paid in full the applicable Fees for Support Services.

2.1 Software Maintenance Services – include each of the following:

Software Updates. During the Support Term , FireEye shall provide Customer notification of bug fixes, maintenance patches and new releases which may contain minor enhancements to the features or functions of the Product ("**Updates**"). FireEye may designate a particular release of the Product as an Update at its sole discretion. Customer may obtain Updates either through delivery of a machine-readable copy pursuant to instructions contained in the document notifying Customer of an available Update or by downloading the Update from FireEye's server via the Internet. FireEye reserves the right to impose additional charges for releases of Products (i) that provide major enhancements to the features or functions of the Products, as determined by FireEye at its sole discretion; or, (ii) that provide additional features or perform additional functions not provided or performed by the Products.

Software Error Corrections. During the Support Term, FireEye shall use commercially reasonable efforts to correct any reproducible programming error in the software associated with the Product attributable to FireEye, employing a level of effort commensurate with the severity of the error, provided, however, that FireEye shall have no obligation to correct all errors in the Products. Upon identification of any programming error, Customer shall notify FireEye of such error in writing and shall provide FireEye with enough information to locate and reproduce the error. FireEye shall not be responsible for correcting any errors not attributable to FireEye. Errors attributable to FireEye shall be those that are reproducible by FireEye on unmodified Products. If it is found that a particular error is fixed in the most current Product release, then FireEye shall have no obligation to fix the error in any prior Product release and Customer will need to upgrade to the current Product release in order to obtain the fix.

2.2 Support Programs

(a) Platinum Support includes all of the services set forth above under Software Maintenance Service (section 2.1) and additionally:

- *Email, Live Chat, Web or Telephone Support*. During the Support Term, FireEye shall provide Customer technical email, live chat, web or telephone support for the Products twenty-four (24) hours per day, 365 days a year. FireEye's support technician shall only be obligated to respond to Customer's fifteen (15) designated contacts.
- FireEye shall use commercially reasonable efforts to respond to the request for support as detailed in the Initial Response Times table found at https://www.fireeye.com/support/programs.html regarding use or installation of the Product that is communicated to FireEye via one of the mechanisms above to the attention of FireEye's support engineers.
- *Product Return*. During the term of this Agreement, Customer shall have the right to return to FireEye any defective Product subject to the limited warranty. Additionally, FireEye will fulfill the following Advance Return provisions below.

- Advance Replacement. Prior to any return as to which Advance Replacement applies, Customer shall verify that said Product is defective by logging a Support request via one of the mechanisms described above and in accordance with FireEye's RMA procedures, including providing the part number, serial number, quantity and reason for return, an explanation of all failure symptoms and other relevant information. Upon confirmation by FireEye of a defect, Customer shall obtain from FireEye an RMA number. FireEye shall ship via a recognized express courier service a replacement Product to Customer to arrive no later than next business day after FireEye's issuance of an RMA number, provided the RMA number was issued prior to the business day cutoff time local to the defective Product, provided the replacement does not require any custom pre-configuration, and provided no external-to-FireEye circumstances prevent the delivery. The replacement Product may be a new or reconditioned Product (of equivalent or better quality) at FireEye's sole discretion. FireEye shall pay the shipping costs to ship the replacement Product to Customer, but Customer shall bear any and all risk of loss of or damage to said Product at all times after said Product is made available by FireEye to the common carrier. The support service will transfer from the defective Product to the replacement Product. Within five (5) business days after Customer receives the replacement Product from FireEye, Customer shall package said defective Product in its original packing material or equivalent, write the RMA number on the outside of the package and return said defective Product, at FireEye's cost provided Customer utilizes FireEye's designated courier service and properly packages the defective Product according to FireEye's instructions, shipped properly insured, FOB FireEye's designated facility (except that FireEye shall pay for shipping). Customer shall enclose with the returned Product the applicable RMA form, and any other documentation or information requested by FireEye customer support. Customer shall assume any and all risk of loss of or damage to such Product during shipping. Title to the defective Product shall pass to FireEye upon FireEye's receipt thereof. When a replacement Product is provided and Customer fails to return the defective Product to FireEye within ten (10) business days after Customer receives the replacement Product from FireEye, FireEye may charge Customer, and Customer shall pay for the replacement Product at the then-current list price.

(b) Platinum Priority Plus Support iincludes all of the services set forth above under Platinum Support [section 2.2(a)] and additionally:

- *Access to Support*. Customer will be provided with direct priority access to Level 2 Advanced Engineering support who shall respond to Customer's unlimited number of designated contacts. A Designated Support Engineer (DSE) point of contact, who is available during Customer's business hours (for single Customer site if Product(s) installed at multiple Customer sites), will be made available to be the focal point of contact within FireEye, to project manage Customer's technical issues.
- *Onsite Support*. Onsite visits for problem assistance at DSE's sole discretion.
- *Reporting*. FireEye will supply Customer with monthly reports detailing technical support provided during the previous month. Quarterly business reviews will also be conducted.

(c) Government Support, if available, includes all of the services set forth above under Platinum Support [section 2.2(a)] and additionally:

- *Email, Live Chat, Web or Telephone Support*. For the specified country, access to citizens of that country for the fulfillment of Level 1 and 2 technical support requests.

(d) Government Priority Plus Support includes all of the services set forth above under Government Support [section 2.2(c)] and additionally:

- *Access to Support*. Customer will be provided with direct priority access to Level 2 Advanced Engineering support who are citizens of that country and shall respond to Customer's unlimited number of designated contacts. A Designated Support Engineer (DSE) point of contact who is a citizen of that country and available during Customer's business hours (for single Customer site if Product(s) installed at multiple Customer sites), will be made available to be the focal point of contact within FireEye, to project manage Customer's technical issues.
- *Onsite Support*. Onsite visits for problem assistance at DSE's sole discretion.
- *Reporting*. FireEye will supply Customer with monthly reports detailing technical support provided during the previous month. Quarterly business reviews will also be scheduled.

(e) Special Services. FireEye agrees to use commercially reasonable efforts to respond to any requests by Customer for support services not specifically provided for above. Customer acknowledges that all such services provided by FireEye shall be at FireEye's discretion and then-current fees and policies.

3. CUSTOMER RESPONSIBILITIES.

3.1 Requesting Support Services. When requesting Support Services from FireEye under this Agreement, Customer should have the following information available to provide to FireEye, if requested: (i) detailed problem description, including operating system ("OS") version, Product model and serial number(s), of the affected Product, and a detailed description of the troubleshooting that has already been done to try to resolve the problem; (ii) detailed system log files; (iii) configuration and login details to allow FireEye access as needed to the Products via the Internet for the purpose of providing support services and permissions needed in order for FireEye to conduct such remote access; (iv) a detailed description of changes to the environment; and (v) Customer's unique ID, Account ID, the serial number(s) of the Product(s) covered by this Agreement or other unique customer identifier as assigned to Customer by FireEye. Customer acknowledges and agrees that failure to have any or all information or access available as needed by FireEye in order to provide the Support Services may result in delays in FireEye's response, may hinder FireEye's ability to perform the Support Services and/or may cause incorrect Support Program fulfillment. FireEye will not be responsible for any such delays and inability to perform due to causes not due to FireEye.

3.2 Customer Assistance. Customer agrees to: (i) ensure that their site complies with any and all applicable FireEye published system environmental specifications; (ii) follow FireEye's procedures when requesting Support Services; (iii) provide FireEye reasonable access to all necessary personnel to answer questions or resolve problems reported by Customer regarding the Products; (iv) promptly implement all Updates and error corrections provided by FireEye under this Agreement; (v) maintain FireEye supported versions of required third party software, if any; and (v) notify FireEye promptly of any relocation of the Products from the location to which the Products were originally shipped. Customer agrees to use reasonable efforts to resolve internally any support questions prior to requesting Support Services pursuant to this Agreement. During the Support Term, FireEye may obtain information regarding Customer's email communication and Customer agrees that, as a condition to FireEye's provision of Support Services, FireEye may use statistical data generated regarding Customer's email correspondence with customer support so long as the source or content of the emails is not being disclosed.

3.3 Contact People. Customer shall appoint the specified number of individuals (depending upon the Support Program purchased) within Customer's organization to serve as contacts between Customer and FireEye and to receive support through FireEye's telephone support center. Customer's contacts shall have been adequately trained on the Products and shall have sufficient technical expertise, training and experience. All of Customer's support inquiries shall be initiated through these contacts.

4. EXCLUSIONS. Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide any Support Services relating to problems arising out of or related to (i) Customer's failure to implement all Updates to the Product which are made available to Customer under this Agreement; (ii) the failure to provide a suitable installation environment; (iii) any alteration, modification, enhancement or addition to the Products performed by parties other than FireEye; (iv) use of the Products in a manner, or for a purpose, for which they were not designed; (v) accident, abuse, neglect, unauthorized repair, inadequate maintenance or misuse of the Products; or relocation of the Products (including without limitation damage caused by use of other than FireEye shipping containers), (vi) operation of the Products outside of environmental specifications; (vii) interconnection of the Products with other products not supplied by FireEye; (viii) use of the Products on any systems other than the specified hardware platform for such Products; or (ix) introduction of data into any database used by the Products by any means other than the use of the software associated with the Products. Notwithstanding anything else contained in this Agreement to the contrary, FireEye will support all generally available ("GA") versions of the FireEye OS, for a minimum of one (1) year from GA release date, regardless of the number of supported OS GA versions. FireEye will also support the two (2) most current OS GA versions, regardless of the elapsed time from GA release date. If available, and at FireEye's sole discretion, support for any other OS versions or for other problems not covered under this Agreement may be obtained at FireEye's then-current fees and policies for such services. FireEye's complete end of life policy can be found at http://www.fireeye.com/support/supported-products.html

5. LAPSED SUPPORT AND UPGRADED SUPPORT.

5.1 Lapsed Support. After any lapse of Support Services, the parties subsequently may elect to reinstate such Support Services for Products for which the Support Services lapsed pursuant to the terms and conditions set forth in this Agreement; provided, however, that (i) Customer agrees to pay for the period of time that has lapsed as well as any renewal term, and (ii) such Products must be in good working condition, as solely determined by FireEye or its designee.

5.2 Support Program Upgrade. At any time during the Term, Customer may upgrade to FireEye's next level of Support Program by (i) notifying FireEye of Customer's desire to upgrade; (ii) acknowledging in writing the then-current terms and conditions for the relevant Support Program; and (iii) paying FireEye the additional Support Fee owed in connection with such upgraded Support Program.

Exhibit A
Product Passthrough Terms – Google Apps for Work (for Customers)

Customer has entered into a certain written agreement (the "Agreement") pursuant to which Customer has purchased the right to access and use the Product. These Product Passthrough Terms set forth the terms and conditions under which Customer may access and use such Product.

1. Product.

   1.1 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Provider stores and processes its own information of a similar type. Provider has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Product, Provider may transfer, store and process Customer Data in the United States or any other country in which Provider or its agents maintain facilities. By using the Product, Customer consents to this transfer, processing and storage of Customer Data.

   1.2 Modifications.

      a. To the Product. Provider may make commercially reasonable changes to the Product, from time to time. If Provider makes a material change to the Product, Customer may be informed of such change, provided that Customer has subscribed with Provider to be informed about such change.

      b. To URL Terms. Provider may make commercially reasonable changes to the URL Terms from time to time. If Provider makes a material change to the URL Terms, Customer may be informed of such change through the Notification Email Address or via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Partner or Provider via the Help Center within thirty days after receiving notice of the change. Upon such notification, Customer will remain governed by the URL Terms in effect immediately prior to the change until the end of the then-current term for the affected Product. If the affected Product is renewed, they will be renewed under Provider's then current URL Terms.

   1.3 Customer Domain Name Ownership. Prior to providing the Product, Provider or Partner may verify that Customer owns or controls the Customer Domain Names. If Customer does not own, or control, the Customer Domain Names, then Provider will have no obligation to provide Customer with the Product.

   1.4 Federal Information Security Management Act (FISMA). The Provider's Product known as "Google Apps Core Services" received a FISMA "Authorization to Operate" for a Moderate impact system. Provider will continue to maintain a System Security Plan (SSP) for the Google Apps Core Services, based on NIST 800-53 Rev. 3, or a similarly applicable standard. If Provider does not maintain this SSP as stated, Customer's sole and exclusive remedy, and Provider's entire liability, will be Customer's ability to terminate use of the Product upon thirty days prior written notice.

2. Customer Obligations.

   2.1 Compliance. Customer will use the Product in accordance with the Acceptable Use Policy. Provider may make new applications, features or functionality for the Product available from time to time, the use of which may be contingent upon Customer's agreement to additional terms. In addition, Provider will make other Non-Google Apps Products (beyond the Product) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Provider terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

   2.2 Customer Administration of the Product. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer and Partner are responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with these

Product Passthrough Terms. Customer agrees that Provider's responsibilities do not extend to the internal management or administration of the Product for Customer and that Provider is merely a data-processor.

2.3 End User Consent. Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Provider providing Customer with the ability to do so, and (ii) Provider to provide the Product.

2.4 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Product, and to terminate any unauthorized use. Customer or Reseller will promptly notify Provider of any unauthorized use of, or access to, the Product of which it becomes aware.

2.5 Restrictions on Use. Unless Provider specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Product to a third party (unless expressly authorized in these Product Passthrough Terms); (b) attempt to reverse engineer the Product or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Product; (d) use the Product for High Risk Activities; or (e) use the Product to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

2.6 Third Party Requests. Customer is responsible for responding to Third Party Requests. Provider will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Provider only if it cannot reasonably obtain such information.

3. Technical Support Services.

3.1 By Customer. Customer or Partner will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Product. Customer or Partner will use commercially reasonable efforts to resolve support issues before escalating them to Provider.

3.2 By Provider. If Customer or Partner cannot resolve a support issue consistent with the above, then Customer or Partner (as applicable based on the agreement between Provider and Partner) may escalate the issue to Provider in accordance with the TSS Guidelines. Provider will provide TSS to Customer or Partner (as applicable) in accordance with the TSS Guidelines.

4. Suspension.

4.1 Of End User Accounts by Provider. If Provider becomes aware of an End User's violation of these Product Passthrough Terms, then Provider may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Provider's request to Suspend an End User Account, then Provider may do so. The duration of any Suspension by Provider will be until the applicable End User has cured the breach which caused the Suspension.

4.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Provider may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Provider Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Provider will provide Customer the reason for the Suspension as soon as is reasonably possible.

5. Confidential Information.

5.1 Obligations. Customer and Provider will: (a) protect the other's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Customer and Provider (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under these Product Passthrough Terms, while using reasonable care to protect it. Customer

and Provider, respectively, will be responsible for any actions of its Affiliates, employees and agents in violation of this Section.

5.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by a third party.

5.3 Required Disclosure. Customer and Provider may disclose the other's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other; and (b) gives the other the chance to challenge the disclosure.

6. Intellectual Property Rights; Brand Features.

6.1 Intellectual Property Rights. Except as expressly set forth herein, these Product Passthrough Terms does not grant either Customer or Provider any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the Customer and Provider, Customer owns all Intellectual Property Rights in Customer Data, and Provider owns all Intellectual Property Rights in the Product.

6.2 Display of Brand Features. Provider may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Product), and within designated areas of the Service Pages. Customer may specify the nature of this use using the Admin Console. Provider may also display Provider Brand Features on the Service Pages to indicate that the Product are provided by Provider. Neither party may display or use the other party's Brand Features beyond what is allowed in these Product Passthrough Terms without the other's prior written consent.

6.3 Brand Features Limitation. Any use of Brand Features will inure to the benefit of the entity holding Intellectual Property Rights in those Brand Features. Any right to use its Brand Features pursuant to these Product Passthrough Terms may be revoked at any time with written notice to the other and a reasonable period to stop the use.

7. Publicity. Customer agrees that Provider may include Customer's name or Brand Features in a list of Provider customers, online or in promotional materials. Customer also agrees that Provider may verbally reference Customer as a customer of the Provider's Product that is the subject of these Product Passthrough Terms.

8. Representations, Warranties and Disclaimers.

8.1 Representations and Warranties. Customer and Provider represent that each will comply with all laws and regulations applicable to its provision, or use, of the Product, as applicable (including applicable security breach notification law). Provider warrants that it will provide the Product in accordance with the applicable SLA.

8.2 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. PROVIDER MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE PRODUCT. CUSTOMER ACKNOWLEDGES THAT THE PRODUCT IS NOT A TELEPHONY SERVICE AND THAT THE PRODUCT IS NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY PRODUCT CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

9. Term and Termination.

9.1 Term. The term for the Product will be as decided upon between Partner and Customer. These Product Passthrough Terms will remain in effect for the Term.

9.2 Termination for Breach. The Services may be suspended or terminated, if: (i) Customer is in material breach of these Product Passthrough Terms and fails to cure that breach within thirty days after receipt of written notice; (ii) Customer ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) Customer is in material breach of these Product Passthrough Terms more than two times notwithstanding any cure of such breaches.

9.3 Effects of Termination. If Services are terminated, then: (i) the rights granted by Provider to Customer, and Customer to Provider will cease immediately (except as set forth in this Section); (ii) neither Customer nor Partner will have access to, or the ability to export, the Customer Data; (iii) Provider will begin to delete Customer Data; and (iv) upon request will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other.

10. Miscellaneous.

10.1 Product Development. The Product was developed solely at private expense and is commercial computer software and related documentation within the meaning of the applicable civilian and military federal acquisition regulations and any supplements thereto.

10.2 Force Majeure. Due to circumstances beyond Provider's controls, Provider may not be able to provide the Product.

10.3 No Waiver. Failure to enforce any provision of these Product Passthrough Terms will not constitute a waiver.

10.4 No Agency. These Product Passthrough Terms do not create any agency, partnership or joint venture.

10.5 No Third-Party Beneficiaries. There are no third-party beneficiaries to these Product Passthrough Terms. Customer's sole remedies will be set forth in its agreement with the Partner.

10.6 Survival. The following sections will survive expiration or termination of these Product Passthrough Terms: Sections 5, 6, 9.3, 10 and 12.

10.7 Severability. If any term (or part of a term) of these Product Passthrough Terms is invalid, illegal, or unenforceable, the rest of these Product Passthrough Terms will remain in effect.

10.8 Conflicting Terms. If there is a conflict between any terms of these Product Passthrough Terms and any other document that makes up the entire agreement as needed for Customer to use the Product, the terms of these Product Passthrough Terms will take precedence.

11. Additional Product Terms.

11.1 Ads. Provider does not serve Ads in the Product or use Customer Data for Ads purposes.

11.2 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Provider may monitor emails sent to these aliases for Customer Domain Names to allow Provider to identify Product abuse.

11.3 Google Apps Vault Retention. If Customer is using Google Apps Vault, Provider will have no obligation to retain any archived Customer Data beyond the retention period specified by Customer. If Customer does not renew Google Apps Vault, Provider will have no obligation to retain any archived Customer Data.

12. Definitions.

"Acceptable Use Policy" means the acceptable use policy for the Product available at http://www.google.com/a/help/intl/en/admins/use_policy.html. The Acceptable Use Policy and such URL link may be updated or modified by Provider from time to time.

"Admin Account(s)" means the administrative account(s) provided to Customer for the purpose of administering the Product. The use of the Admin Account(s) requires a password, which Provider will provide to Customer or Partner.

"Admin Console" means the online tool Customer may use in reporting and certain other administration functions.

"Administrators" mean the Customer-designated technical personnel who administer the Product to End Users on Customer's behalf.

"Ads" means online advertisements displayed by Provider to End Users, excluding advertisements provided by any advertising products that are not part of the Product that Customer chooses to use in connection with the Product.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with an entity.

"Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured from time to time.

"Confidential Information" means information disclosed or exchanged under these Product Passthrough Terms that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is Customer's Confidential Information.

"Customer Data" means data, including email, provided, generated, transmitted or displayed via the Product by Customer, End Users, or Partner on behalf of Customer.

"Customer Domain Names" mean the domain names owned or controlled by Customer, which will be used in connection with the Product.

"Emergency Security Issue" means either: (a) Customer's use of the Product in violation of the Acceptable Use Policy, which could disrupt: (i) the Product; (ii) other customers' use of the Product; or (iii) the Provider network or servers used to provide the Product; or (b) unauthorized third party access to the Product.

"End Users" means the individuals Customer permits to use the Product.

"End User Account" means a Provider-hosted account established by Customer through the Product for an End User.

"Export Control Laws" means all applicable export and reexport control laws and regulations, including trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State.

"Google Apps Core Services" means the applicable Product purchased by Customer from Partner which are more fully described here: http://www.google.com/a/help/intl/en/users/user_features.html. The Google Apps Core Services and such URL link may be updated or modified by Provider from time to time.

"Help Center" means the Provider help center accessible at http://www.google.com/support/. The Help Center and such URL link may be updated or modified by Provider from time to time.

"High Risk Activities" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Product could lead to death, personal injury, or environmental damage.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

"Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

"Non-Google Apps Products" means Provider products which are not part of the Product, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865. The Non-Google Apps Products and such URL link may be updated or modified by Provider from time to time.

"Non-Google Apps Product Terms" means the terms found at the following URL: http://www.google.com/apps/intl/en/terms/additional_services.html. The Non-Google Apps Product Terms and such URL link may be updated or modified by Provider from time to time.

"Notification Email Address" means the email address designated by Customer to receive email notifications from Provider. Customer may provide a Partner email address for this purpose if it so chooses. Customer may change this email address through the Admin Console.

"Provider" means the third party provider of the Product.

"Partner" means the entity Customer is paying to provide access to and use of the Product.

"Service Pages" mean the web pages displaying the Product to End Users.

"Product" means, as applicable, the Google Apps Core Services purchased from Partner.

"SLA" means the Service Level Agreement located here for applicable Google Apps Core Services: http://www.google.com/apps/intl/en/terms/reseller_sla.html. The SLA and such URL link may be updated or modified by Provider from time to time.

"Suspend" means the immediate disabling of access to the Product, or components of the Product, as applicable, to prevent further use of the Product.

"Term" means the term of these Product Passthrough Terms, which will continue for as long as Customer is receiving Product from Provider, unless terminated earlier pursuant to these Product Passthrough Terms, or pursuant to Customer's agreement with Partner.

"Third Party Request" means a request from a third party for records relating to an End User's use of the Product. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"TSS" means the technical support Product provided by Provider to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Provider's technical support Product guidelines then in effect for the Product. TSS Guidelines are at the following URL: http://www.google.com/a/help/intl/en/admins/tssg.html. The TSS Guidelines and such URL link may be updated or modified by Provider from time to time.

"URL Terms" means the Acceptable Use Policy, the SLA and the TSS Guidelines.

SALESFORCE Service Terms

"AppExchange" means the online directory of on-demand applications that work with the Service, located at http://www.appexchange.com or at any successor websites.

"Service" means the online, Web-based application provided by Salesforce.com (sometimes referred to as "SFDC") via http://www.salesforce.com and/or other designated websites, including associated offline components but excluding AppExchange applications.

"Third-Party Applications" means online, Web-based applications and offline software products that are provided by third parties, interoperate with the Service, and are identified as third-party applications, including but not limited to those listed on the AppExchange.

"User Guide" means the online user guide for the Services, accessible via http://www.salesforce.com, as updated from time to time.

"Users" means Your employees, representatives, consultants, contractors or agents who are authorized to use the Service and have been supplied user identifications and passwords by You (or by Salesforce.com or Your reseller at Your request).

"You" and **"Your"** means the customer entity which has contracted to purchase subscriptions to use the Service subject to the conditions of these SFDC Service Terms.

"**Your Data**" means all electronic data or information submitted by You to the Service.

1. **Use of Service**

(a) User subscriptions cannot be shared or used by more than one User (but may be reassigned from time to time to new Users who are replacing former Users who have terminated employment with You or otherwise changed job status or function and no longer require use of the Service).

(b) You (i) are responsible for all activities occurring under Your User accounts; (ii) are responsible for the content of all Your Data; (iii) shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Service, and shall notify Your reseller or Salesforce.com promptly of any such unauthorized use You become aware of; and (iv) shall comply with all applicable federal laws and regulations in using the Service.

(c) You shall use the Service solely for Your internal business purposes and shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Service available to any third party, other than to Users or as otherwise contemplated by these SFDC Service Terms; (ii) send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (iii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or violates third party privacy rights; (iv) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs; (v) interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (vi) attempt to gain unauthorized access to the Service or its related systems or networks.

(d) You shall not (i) modify, copy or create derivative works based on the Service; (ii) frame or mirror any content forming part of the Service, other than on Your own intranets or otherwise for its own internal business purposes; (iii) reverse engineer the Service; or (iv) access the Service in order to (A) build a competitive product or service, or (B) copy any ideas, features, functions or graphics of the Service.

2. **Service Provision.** Salesforce.com will use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which SFDC shall give at least 8 hours notice via the Services and which SFDC shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday), or (b) any unavailability caused by circumstances beyond SFDC's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving SFDC employees), or Internet service provider failures or delays.

Salesforce.com will provide the Services only in accordance with applicable laws and government regulations.

3. **Acquisition of Third-Party Products and Services.** Any acquisition by You of third-party products or services, including but not limited to Third-Party Applications and implementation, customization and other consulting services, and any exchange of data between You and any third-party provider, is solely between You and the applicable third-party provider. Salesforce.com does not warrant or support third-party products or services, whether or not they are designated by Salesforce.com as "certified" or otherwise. No purchase of third-party products or services is required to use the Service as provided by Salesforce.com.

4. **Third-Party Applications and Your Data.** If You install or enable Third-Party Applications for use with the Service, You acknowledge that Salesforce.com may allow providers of those Third-Party Applications to access You Data as required for the interoperation of such Third Party Applications with the Service. Salesforce.com shall not be responsible for any disclosure, modification or deletion of You Data resulting from any such access by Third-Party Application providers. The Service shall allow You to restrict such access by restricting Users from installing or enabling such Third-Party Applications for use with the Service.

5. **Google Services.** Service features that interoperate with Google services depend on the continuing availability of the Google application programming interface ("API") and program for use with the Service. If Google Inc. ceases to make the Google API or program available on reasonable terms for the Service, Salesforce.com may cease providing such Service features without entitling You to any refund, credit, or other compensation.

6. **Proprietary Rights.** Subject to the limited rights expressly granted hereunder, Salesforce.com reserves all rights, title and interest in and to the Service, including all related intellectual property rights. The Service is deemed Salesforce.com confidential information, and You will not use it or disclose it to any third party except as permitted in these SFDC Service Terms and except as required by law, upon notice to Salesforce.com.

7. **Your Data.** As between Salesforce.com and You, You exclusively own all rights, title and interest in and to all of Your Data. Your Data is deemed your confidential information, and Salesforce.com shall not access Your User accounts, including Your Data, except to respond to service or technical problems or at your request.

8. **Compelled Disclosure.** If either You or Salesforce.com is compelled by law to disclose confidential information of the other party, it shall provide the other party with prior notice of such

compelled disclosure (to the extent legally permitted) and reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.

9. **Suggestions** You agree that Salesforce.com shall have a royalty-free, worldwide, transferable, sublicenseable, irrevocable, perpetual license to use or incorporate into the Service any suggestions, enhancement requests, recommendations or other feedback provided by You or Your Users relating to the operation of the Service.

10. **Fees.** Contracted for fees for use of the Service represent a firm commitment and the number of User subscriptions contracted for cannot be reduced in the middle of a subscription term.

11. **Termination.** The master contract governs your termination (FAR 52.212-4(l) & (m)) and cancellation rights with the contractor, and the contract requires continued performance while any disputes are resolved (FAR 52.233-1(i)).

12. **Data Storage.** You are entitled to a cumulative amount of storage per User subscription for no additional charge as set forth in the User Guide for the Service subscription type purchased. You may purchase additional storage if necessary, and you may contact Your reseller for then-current rates listed in master contract price list.

13. **Support.** SFDC will provide You with basic support as described from time to time by SFDC at www.salesforce.com. In the event that You have purchased an upgraded support package, then upgraded support contact information will be provided to You together with your initial account set up information.

14. **No Warranty.** SALESFORCE.COM MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE AND/OR SUPPORT, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. IN THE EVENT THAT YOUR AGREEMENT WITH YOUR RESELLER PROVIDES ANY WARRANTIES WITH RESPECT TO THE SERVICE AND/OR SUPPORT, SUCH WARRANTIES ARE SOLELY BETWEEN YOU AND YOUR RESELLER. This clause does not disclaim any warranties expressly provided in a contract with the U.S. Government."

15. **No Liability.** IN NO EVENT SHALL SALESFORCE.COM HAVE ANY LIABILITY TO YOU OR ANY USER FOR ANY DAMAGES WHATSOVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT EITHER YOU OR SALESFORCE.COM HAVE BEEN ADVISED OF THE POSSIBILI TY OF SUCH DAMAGES. This clause shall not impair the

U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to EXPRESS remedies provided in the Contract (i.e. clause 552.238-72 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, Liability for Injury or Damage (Section 3 of the Price List), and GSAR 552.215-72 – Price Adjustment – Failure to Provide Accurate Information).

16. **Further Contact.** Salesforce.com may contact you regarding new Salesforce.com service features and offerings.

17. **Third Party Beneficiary.** SFDC shall be a third party beneficiary to the agreement between You and Reseller solely as it relates to these SFDC Service Terms.

SOFTWARE LICENSE AND SUPPORT AGREEMENT
General Terms and Conditions
("GTC")

1. DEFINITIONS.

1.1 "Add-on" means any development using SAP API's that adds new and independent functionality, but does not modify existing SAP functionality.

1.2 "Agreement" means these GTCs, any Order Form referencing these GTCs, and the Use Terms and Schedules referenced by these GTCs and/or such Order Forms. All such components are integral to the agreement, and collectively are referred to herein as the "Agreement".

1.3 "API" means SAP's application programming interfaces, as well as other SAP code that allow other software products to communicate with or call on SAP Software (for example, SAP Enterprise Services, BAPIs, Idocs, RFCs and ABAP or other user exits) provided under this Agreement.

1.4 "Affiliate" mean any legal entity in the Territory in which the Licensee, directly or indirectly, holds more than fifty percent (50%) of the shares or voting rights. Any such legal entity shall be considered an Affiliate for only such time as such equity interest is maintained.

1.5 "Business Partner" means a legal entity that requires access to the Software in connection with Licensee's internal business operations, such as customers, distributors and/or suppliers of Licensee.

1.6 "Confidential Information" means, with respect to SAP, all information which SAP protects against unrestricted disclosure to others, including but not limited to: (a) the Software and Documentation and other SAP Materials, including without limitation the following information regarding the Software: (i) computer software (object and source codes), programming techniques and programming concepts, methods of processing, system designs embodied in the Software; (ii) benchmark results, manuals, program listings, data structures, flow charts, logic diagrams, functional specifications, file formats; and (iii) discoveries, inventions, concepts, designs, flow charts, documentation, product specifications, application program interface specifications, techniques and processes relating to the Software; (b) the research and development or investigations of SAP; (c) product offerings, content partners, product pricing, product availability, technical drawings, algorithms, processes, ideas, techniques, formulas, data, schematics, trade secrets, know-how, improvements, marketing plans, forecasts and strategies; and (d) any information about or concerning any third party (which information was provided to SAP subject to an applicable confidentiality obligation to such third party). With respect to Licensee, "Confidential Information" means all information which Licensee protects against unrestricted disclosure to others and which (i) if in tangible form, Licensee clearly identifies as confidential or proprietary at the time of disclosure; and (ii) if in intangible form (including disclosure made orally or visually), Licensee identifies as confidential at the time of disclosure, summarizes the Confidential Information in writing, and delivers such summary within thirty (30) calendar days of any such disclosure.

1.7 "Documentation" means SAP's documentation which is delivered or made available to Licensee with the Software under this Agreement.

1.8 "Intellectual Property Rights" means patents of any type, design rights, utility models or other similar invention rights, copyrights, mask work rights, trade secret or confidentiality rights, trademarks, trade names and service marks and any other intangible property rights, including applications and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, now existing or hereafter filed, issued, or acquired.

1.9 "Modification" means (i) a change to the delivered source code or metadata; or (ii) any development, other than a change to the delivered source code or metadata, that customizes, enhances, or changes existing functionality of the Software including, but not limited to, the creation of any new application program interfaces, alternative user interfaces or the extension of SAP data structures; or (iii) any other change to the Software (other than an Add-on) utilizing or incorporating any SAP Materials (defined below).

1.10 "Professional Services Schedule" means the terms and conditions governing SAP's delivery of professional services, attached hereto and made a part hereof.

1.11 "SAP Materials" means any software, programs, tools, systems, data, or other materials made available by SAP to Licensee in the course of the performance under this Agreement including, but not limited to, the Software and Documentation, as well as any information, materials or feedback provided by Licensee to SAP relating to the Software and Documentation.

1.12 "SAP Support" means SAP's then-current SAP support offering specified in the applicable Order Forms and made available to Licensee as stated in the applicable SAP Support Schedule found at www.sap.com/company/legal/index.epx as of the effective date of the first Software Order Form issued under these GTCs. Such SAP Support Schedule is incorporated herein by reference. For the avoidance of doubt, such SAP Support Schedule shall apply to all Order Forms issued under these GTCs, unless otherwise agreed by the parties. SAP recommends Licensee prints a copy of the applicable SAP Support Schedule for Licensee's own records.

1.13 "Software" means (i) any and all software products licensed to Licensee under this Agreement as specified in Software Order Forms hereto, all as developed by or for SAP, SAP AG, Business Objects Software Limited and/or any of their affiliated companies and delivered to Licensee hereunder; (ii) any new releases thereof made available through unrestricted shipment pursuant to the respective support agreement and (iii) any complete or partial copies of any of the foregoing.

1.14 "Software Order Form" means the order form for the Software and related SAP Support ordered by Licensee thereunder, including information on Software, SAP Support, fees, and other information necessary for the delivery of such items to Licensee.

The Software Order Form does not include fees for professional services, which shall be billed under separate statements of work in accord with the Professional Services Schedule.

1.15 "Territory" means the world except for those countries prohibited by United States' export laws, and further subject to Section 12.4 of the GTC.

1.16 "Third Party Software" means (i) any and all software products and content licensed to Licensee under this Agreement as specified in Software Order Forms hereto, all as developed by companies other than SAP, SAP AG, Business Objects Software Limited and/or any of their affiliated companies and delivered to Licensee hereunder; (ii) any new releases thereof made available through unrestricted shipment pursuant to the respective SAP Support Schedule and (iii) any complete or partial copies of any of the foregoing.

1.17 "Use" means to activate the processing capabilities of the Software, load, execute, access, employ the Software, or display information resulting from such capabilities.

1.18 "Use Terms" means, with regard to Software specified in a Software Order Form, the SAP Software Use Rights document current at the time of execution of such Software Order Form, copies of which are found at www.sap.com/company/legal/index.epx and made a part hereof. Such SAP Software Use Rights documents are incorporated herein by reference. SAP recommends Licensee prints copies of the applicable SAP Software Use Rights documents for Licensee's own records

2. LICENSE GRANT.

2.1 License.

2.1.1 Subject to Licensee's compliance with all the terms and conditions of this Agreement, SAP grants to Licensee a non-exclusive, perpetual (except for subscription based or term licenses) license to Use the Software, Documentation, and other SAP Materials at specified site(s) within the Territory to run Licensee's and its Affiliates' internal business operations (including customer back-up and passive disaster recovery) and to provide internal training and testing for such internal business operations and as further set forth in the Software Order Form, unless terminated in accordance with Section 5 herein. This license does not permit Licensee (without being limited specifically to such restrictions) to: (i) use the SAP Materials to provide services to third parties (e.g., business process outsourcing, service bureau applications or third party training) other than to Affiliates (subject to Section 2.2); (ii) lease, loan, resell, sublicense or otherwise distribute the SAP Materials, other than distribution to Affiliates (subject to Section 2.2); (iii) make any Use of or perform any acts with respect to the SAP Materials other than as expressly permitted in accordance with the terms of this Agreement; or (iv) use Software components other than those specifically identified in the Software Order Form, even if it is also technically possible for Licensee to access other Software components. Business Partners may Use the Software only through screen access and solely in conjunction with Licensee's Use and may not Use the Software to run any of Business Partners' business operations.

2.1.2 Licensee agrees to install the Software only on information technology devices (e.g. hard disks or central processing units) identified by Licensee pursuant to this Agreement and that has been previously approved by SAP in writing or otherwise officially made known to the public as appropriate for Use or interoperation with the Software (the "Designated Unit"). Licensee must hold the required licenses as stated herein and in the applicable Order Forms, for any individuals that Use the Software, including employees or agents of Affiliates and Business Partners. Use may occur by way of an interface delivered with or as a part of the Software, a Licensee or third-party interface, or another intermediary system.

2.1.3 The terms and conditions of this Agreement relative to "Software" apply to Third Party Software except as otherwise stated in the Software Use Rights Schedule, a Schedule, an Order Form, or an Amendment.

2.2 Affiliate Use. Affiliates' Use of the Software, Documentation and other SAP Materials to run their internal business operations as permitted under Section 2.1.1 is subject to the following: (i) the Affiliate agrees to be bound by the terms herein in the form of Schedule A ("Affiliate Use Agreement") attached hereto; and (ii) a breach of such Affiliate Use Agreement by Affiliate shall be considered a breach by Licensee hereunder. If Licensee has an affiliate or subsidiary with a separate agreement for SAP software licenses and/or support services with SAP AG, any SAP AG affiliate (including SAP) or any other distributor of SAP software, the Software shall not be Used to run such affiliate's or subsidiary's business operations and such affiliate or subsidiary shall not receive any support services under this Agreement even if such separate agreement has expired or is terminated, unless otherwise agreed to in writing by the parties.

2.3 Outsourcing Services. With SAP's prior written consent, Licensee may permit services providers to access the Software solely for the purpose of providing facility, implementation, systems, application management or disaster recovery services to Licensee in connection with the business of Licensee for which the Software is herein licensed provided: (i) Licensee and such services provider execute a written agreement that includes provisions requiring such services provider's compliance with the terms of this Agreement prior to such access, including without limitation non-disclosure of SAP Confidential Information; (ii) Licensee shall hold the required licenses as stated in the Use Terms for all employees of such services provider authorized to access the Software; (iii) such services provider shall be permitted to Use the Software solely to install and configure the Software in accordance with the business of Licensee as set forth herein (or in the case of a disaster recovery vendor, to provide disaster recovery services only); (iv) under no circumstances may such services provider Use the Software to operate or provide processing services to Licensee or any other party, or in connection with such services provider's own business operations; (v) Licensee shall be responsible for any additional Software, migration tools, or third party software needed to effect such transition; and (vi) Licensee expressly agrees to indemnify SAP, its officers, employees, agents and subcontractors from and against all claims, liabilities, losses, damages and costs (including reasonable attorney fees) suffered by SAP arising from a breach by the services provider of the conditions of this Agreement. Upon SAP request, Licensee shall provide written confirmation to SAP that items (i)-(iv) are fulfilled.

3. VERIFICATION. SAP shall be permitted to audit (at least once annually and in accordance with SAP standard procedures, which may include on-site and/or remote audit) the usage of the SAP Materials. Licensee shall cooperate reasonably in the conduct of such audits. In the event an audit reveals that (i) Licensee underpaid license fees and/or SAP Support fees to SAP and/or (ii) that Licensee has Used the Software in excess of the license quantities or levels stated in the Software Order Form, Licensee shall pay such underpaid fees and/or for such excess usage based on SAP List of Prices and Conditions Software and Support governing use in effect at the time of the audit, and shall execute an additional Software Order Form in accordance with the terms of this Agreement

to affect the required licensing of any additional quantities or levels. Reasonable costs of SAP's audit shall be paid by Licensee if the audit results indicate usage in excess of the licensed quantities or levels. SAP reserves all rights at law and equity with respect to both Licensee's underpayment of License fees or SAP Support fees and usage in excess of the license quantities or levels.

4. PRICE, PAYMENT, AND DELIVERY.

4.1 Fees. Licensee shall pay to SAP license fees for the Software and fees for SAP Support on the terms in Software Order Forms hereto. Fees for consulting services will be paid as set forth in the Professional Services Schedule. Any fees not paid when due shall accrue interest at the rate of 18% (eighteen percent) per annum, but not to exceed the maximum amount as allowed by law.

4.2 Taxes. Fees and other charges described in this Agreement do not include federal, state or local sales, foreign withholding, use, property, excise, service, or similar transaction taxes ("Tax(es)") now or hereafter levied, all of which shall be for Licensee's account. Any applicable direct pay permits or valid tax-exempt certificates must be provided to SAP prior to the execution of this Agreement. If SAP is required to pay Taxes, Licensee shall reimburse SAP for such amounts. Licensee hereby agrees to indemnify SAP for any Taxes and related costs, interest and penalties paid or payable by SAP.

4.3 Delivery of the Software and SAP Support. SAP will deliver the Software and SAP Support by making it available for electronic download through the SAP ServiceMarketplace (http://service.sap.com/swdc) to Licensee. Risk of loss passes at the time of such electronic delivery. Licensee agrees not to request any physical delivery of Software or SAP Support and should it occur that any such delivery will be rejected by Licensee. Licensee agrees and understands that the calculation of Taxes may be affected by the delivery method and delivery location of the Software and corresponding SAP Support.

5. TERM.

5.1. Term. This Agreement and the license granted hereunder shall become effective as of the date first set forth in the first Software Order Form issued under these GTCs, and shall continue in effect thereafter unless this Agreement is terminated upon the earliest to occur of the following: (i) thirty days after Licensee gives SAP written notice of Licensee's direction to terminate this Agreement, for any reason, but only after payment of all license and SAP Support fees then due and owing; (ii) thirty days after SAP gives Licensee notice of Licensee's material breach of any provision of the Agreement (other than Licensee's breach of its obligations under Sections 6, 10 or 11, which breach shall result in immediate termination), including more than thirty days delinquency in Licensee's payment of any money due hereunder, unless Licensee has cured such breach during such thirty day period; (iii) immediately if Licensee files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors. For the avoidance of any doubt, termination of the Agreement shall strictly apply to all licenses under the Agreement, its appendices, schedules, addenda and order documents and any partial termination of the Agreement by Licensee shall not be permitted in respect of any part of the Agreement, its appendices, schedules, addenda, order documents.

5.2 End of Term Duties. Upon any termination hereunder, Licensee and its Affiliates shall immediately cease Use of all SAP Materials and Confidential Information. Within thirty (30) days after any termination, Licensee shall irretrievably destroy or upon SAP's request deliver to SAP all copies of the SAP Materials and Confidential Information in every form, except to the extent it is legally required to keep it for a longer period in which case such return or destruction shall occur at the end of such period. Licensee must certify to SAP in writing that it has satisfied its obligations under this Section 5.2. Licensee agrees to certify in writing to SAP that it and each of its Affiliates has performed the foregoing. Sections 3, 4, 5.2, 6, 7.2, 8, 9, 10, 12.4, 12.5, 12.6 and 12.8 shall survive such termination. In the event of any termination hereunder, Licensee shall not be entitled to any refund of any payments made by Licensee. Termination shall not relieve Licensee from its obligation to pay fees that remain unpaid.

6. INTELLECTUAL PROPERTY RIGHTS.

6.1 Reservation of Rights. The SAP Materials, and all Intellectual Property Rights embodied in the foregoing, shall be the sole and exclusive property of SAP, SAP AG (the parent company of SAP) or its or their licensors, subject to any rights expressly granted to Licensee in Section 2 and 6.3 herein. Except for the rights set forth in Section 6.3 herein, Licensee is not permitted to modify or otherwise make derivative works of the Software. Any such unauthorized works developed by Licensee, and any Intellectual Property Rights embodied therein, shall be the sole and exclusive property of SAP or SAP AG.

6.2 Protection of Rights. Licensee shall not copy, translate, disassemble, or decompile, nor create or attempt to create the source code from the object code of the Software in any manner. Reverse engineering of the Software and other SAP Materials is prohibited. Licensee is permitted to back up data in accordance with good information technology practice and for this purpose to create the necessary backup copies of the Software. Backup copies on transportable discs or other data media must be marked as backup copies and bear the same copyright and authorship notice as the original discs or other data media. Licensee must not change or remove SAP's copyright and authorship notices.

6.3 Modifications/Add-ons.

6.3.1 Conditioned on Licensee's compliance with the terms and conditions of this Agreement, Licensee may make Modifications and/or Add-ons to the Software in furtherance of its permitted Use under this Agreement, and shall be permitted to use Modifications and Add-ons with the Software in accordance with the License grant to the Software set forth in Section 2.1.1 herein. Licensee shall comply with SAP's registration procedure prior to making Modifications or Add-ons. All Modifications and all rights associated therewith shall be the exclusive property of SAP and SAP AG. All Add-ons developed by SAP (either independently or jointly with Licensee) and all rights associated therewith shall be the exclusive property of SAP and SAP AG. Licensee agrees to execute those documents reasonably necessary to secure SAP's rights in the foregoing. All Add-ons developed by or on behalf of Licensee without SAP's participation ("Licensee Add-on"), and all rights associated therewith, shall be the exclusive property of Licensee subject to SAP's rights in and to the Software; provided, Licensee shall not commercialize, market, distribute, license, sublicense, transfer, assign or otherwise alienate any such Licensee Add-ons. SAP retains the right to independently develop its own Modifications or Add-ons to the Software, and Licensee agrees not to take any action that would limit SAP's sale, assignment, licensing or use of its own Software or Modifications or Add-ons thereto.

6.3.2 Any Modification developed by or on behalf of Licensee without SAP's participation or Licensee Add-on must not (and subject to other limitations set forth herein): enable the bypassing or circumventing any of the restrictions set forth in this Agreement and/or provide Licensee with access to the Software to which Licensee is not directly licensed; nor permit mass data extraction from

Software to any non-SAP software, including use, modification saving or other processing of data in the non-SAP software; nor unreasonably impair, degrade or reduce the performance or security of the Software; nor render or provide any information concerning SAP software license terms, Software, or any other information related to SAP products.

6.3.3 Licensee covenants, on behalf of itself and its successors and assigns, not to assert against SAP or its affiliated companies, or their resellers, distributors, suppliers, commercial partners and customers, any rights in any Modifications developed by or on behalf of Licensee without SAP participation or Licensee Add-ons , or any other functionality of the SAP Software accessed by such Modification developed by or on behalf of Licensee without SAP participation or Licensee Add-on.

7. PERFORMANCE WARRANTY.

7.1 Warranty. SAP warrants that the Software will substantially conform to the specifications contained in the Documentation for six months following delivery. The warranty shall not apply: (i) if the Software is not used in accordance with the Documentation; or (ii) if the defect is caused by a Modification or Add-on (other than a Modification or Add-on made by SAP and which is provided through SAP Support or under warranty), Licensee or third-party software. SAP does not warrant that the Software will operate uninterrupted or that it will be free from minor defects or errors that do not materially affect such performance, or that the applications contained in the Software are designed to meet all of Licensee's business requirements. Provided Licensee notifies SAP in writing with a specific description of the Software's nonconformance within the warranty period and SAP validates the existence of such nonconformance, SAP will, at its option: a) repair or replace the nonconforming Software, or b) refund the license fees paid for the applicable nonconforming Software in exchange for a return of such nonconforming Software. This is Licensee's sole and exclusive remedy under this warranty.

7.2 Express Disclaimer. SAP AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

8. INDEMNIFICATION.

8.1 Infringement and Defense of Licensee. SAP shall defend Licensee against claims brought against Licensee in the Territory by any third party alleging that Licensee's Use of the Software, in accordance with the terms and conditions of this Agreement, constitutes a direct infringement or misappropriation of a patent claim(s), copyright or trade secret rights, and SAP will pay damages finally awarded against Licensee (or the amount of any settlement SAP enters into) with respect to such claims. This obligation of SAP shall not apply if the alleged infringement or misappropriation results from Use of the Software in conjunction with any other software, an apparatus other than a Designated Unit, failure to use an update promptly provided by SAP if such infringement or misappropriation could have been avoided by use of the update, or unlicensed activities. This obligation of SAP also shall not apply if Licensee fails to timely notify SAP in writing of any such claim. SAP is permitted to control fully the defense and any settlement of any such claim as long as such settlement shall not include a financial obligation on Licensee. In the event Licensee declines SAP's proffered defense, or otherwise fails to give full control of the defense to SAP's designated counsel, then Licensee waives SAP's obligations under this Section 8.1. Licensee shall cooperate fully in the defense of such claim and may appear, at its own expense, through counsel reasonably acceptable to SAP. SAP expressly reserves the right to cease such defense of any claim(s) in the event the Software is no longer alleged to infringe or misappropriate, or is held not to infringe or misappropriate, the third party's rights. SAP may settle or mitigate damages arising from any claim or potential claim, by substituting alternative substantially equivalent non-infringing programs and supporting documentation for the Software. Licensee shall not undertake any action in response to any infringement or misappropriation, or alleged infringement or misappropriation of the Software that is prejudicial to SAP's rights.

8.2 THE PROVISIONS OF THIS SECTION 8 STATE THE SOLE, EXCLUSIVE, AND ENTIRE LIABILITY OF SAP AND ITS LICENSORS TO LICENSEE, AND IS LICENSEE'S SOLE REMEDY, WITH RESPECT TO THE INFRINGEMENT OR MISAPPROPRIATION OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

9. LIMITATIONS OF LIABILITY.

9.1 Not Responsible. SAP and its licensors will not be responsible under this Agreement (i) if the Software is not used in accordance with the Documentation; or (ii) if the defect or liability is caused by Licensee, a Modification or Add-on (other than a Modification or Add-on made by SAP which is provided through SAP Support or under warranty), or third-party software. SAP AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY CLAIMS OR DAMAGES ARISING FROM INHERENTLY DANGEROUS USE OF THE SOFTWARE AND/OR THIRD-PARTY SOFTWARE LICENSED HEREUNDER.

9.2 Exclusion of Damages; Limitation of Liability. ANYTHING TO THE CONTRARY HEREIN NOTWITHSTANDING, EXCEPT FOR DAMAGES RESULTING FROM UNAUTHORIZED USE OR DISCLOSURE OF CONFIDENTIAL INFORMATION OR DEATH OR PERSONAL INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL SAP, ITS LICENSORS OR LICENSEE BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE PAID LICENSE FEES FOR THE SOFTWARE DIRECTLY CAUSING THE DAMAGES OR BE LIABLE IN ANY AMOUNT FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES, LOSS OF GOOD WILL OR BUSINESS PROFITS, WORK STOPPAGE, DATA LOSS, COMPUTER FAILURE OR MALFUNCTION, ATTORNEYS' FEES, COURT COSTS, INTEREST OR EXEMPLARY OR PUNITIVE DAMAGES. The provisions of this Agreement allocate the risks between SAP and Licensee. The license fees reflect this allocation of risk and the limitations of liability herein.

10. CONFIDENTIALITY.

10.1. Use of Confidential Information. Confidential Information shall not be reproduced in any form except as required to accomplish the intent of this Agreement. Any reproduction of any Confidential Information of the other shall remain the property of the disclosing party and shall contain any and all confidential or proprietary notices or legends which appear on the original. With respect to the Confidential Information of the other, each party : (a) shall take all Reasonable Steps (defined below) to keep all Confidential Information strictly confidential; and (b) shall not disclose any Confidential Information of the other to any person other than its bona fide individuals whose access is necessary to enable it to exercise its rights hereunder. As used herein "Reasonable Steps" means those steps the receiving party takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care. Confidential Information of either party disclosed prior to execution of this Agreement shall be subject to the protections afforded hereunder.

10.2 Exceptions. The above restrictions on the use or disclosure of the Confidential Information shall not apply to any Confidential Information that: (a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information, or is lawfully received free of restriction from a third party having the right to furnish such Confidential Information; (b) has become generally available to the public without breach of this Agreement by the receiving party; (c) at the time of disclosure, was known to the receiving party free of restriction; or (d) the disclosing party agrees in writing is free of such restrictions.

10.3 Confidential Terms and Conditions; Publicity. Licensee shall not disclose the terms and conditions of this Agreement or the pricing contained therein to any third party. Neither party shall use the name of the other party in publicity, advertising, or similar activity, without the prior written consent of the other, except that Licensee agrees that SAP may use Licensee's name in customer listings or, at times mutually agreeable to the parties, as part of SAP's marketing efforts (including without limitation reference calls and stories, press testimonials, site visits, SAPPHIRE participation).

11. ASSIGNMENT. Licensee may not, without SAP's prior written consent, assign, delegate, pledge, or otherwise transfer this Agreement, or any of its rights or obligations under this Agreement, or the SAP Materials or SAP Confidential Information, to any party, whether voluntarily or by operation of law, including by way of sale of assets, merger or consolidation. SAP may assign this Agreement to any of its affiliates.

12. GENERAL PROVISIONS.

12.1 Severability. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such invalidity or unenforceability shall not affect the other provisions of this Agreement, and this Agreement shall be construed as if such invalid or unenforceable provision had never been contained herein.

12.2 No Waiver. If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

12.3 Counterparts. This Agreement may be signed in two counterparts, each of which shall be deemed an original and which shall together constitute one Agreement.

12.4 Regulatory Matters. The Software, Documentation and SAP Materials are subject to the export control laws of various countries, including without limit the laws of the United States and Germany. Licensee agrees that it will not submit the Software, Documentation or other SAP Materials to any government agency for licensing consideration or other regulatory approval without the prior written consent of SAP, and will not export the Software, Documentation and SAP Materials to countries, persons or entities prohibited by such laws. Licensee shall also be responsible for complying with all applicable governmental regulations of the country where Licensee is registered, and any foreign countries with respect to the use of the Software, Documentation or other SAP Materials by Licensee and/or its Affiliates.

12.5 Governing Law; Limitations Period. This Agreement and any claims arising out of or relating to this Agreement and its subject matter shall be governed by and construed under the laws of Commonwealth of Pennsylvania without reference to its conflicts of law principles. In the event of any conflicts between foreign law, rules, and regulations, and United States law, rules, and regulations, United States law, rules, and regulations shall prevail and govern. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. The Uniform Computer Information Transactions Act as enacted shall not apply. Licensee must initiate a cause of action for any claim(s) arising out of or relating to this Agreement and its subject matter within one (1) year from the date when Licensee knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

12.6 Notices. All notices or reports which are required or may be given pursuant to this Agreement shall be in writing and shall be deemed duly given when delivered to the respective executive offices of SAP and Licensee at the addresses first set forth in any Software Order Form. Where in this section 12.6 or elsewhere in this Agreement written form is required, that requirement can be met by facsimile transmission, exchange of letters or other written form.

12.7 Force Majeure. Any delay or nonperformance of any provision of this Agreement (other than for the payment of amounts due hereunder) caused by conditions beyond the reasonable control of the performing party shall not constitute a breach of this Agreement, and the time for performance of such provision, if any, shall be deemed to be extended for a period equal to the duration of the conditions preventing performance.

12.8 Entire Agreement. This Agreement constitutes the complete and exclusive statement of the agreement between SAP and Licensee, and all previous representations, discussions, and writings are merged in, and superseded by this Agreement and the parties disclaim any reliance on any such representations, discussions and writings. This Agreement may be modified only by a writing signed by both parties. This Agreement shall prevail over any additional, conflicting, or inconsistent terms and conditions which may appear on any purchase order or other document furnished by Licensee to SAP. This Agreement shall prevail over any additional, conflicting or inconsistent terms and conditions which may appear in any clickwrap end user agreement included in the Software. Signatures sent by electronic means (facsimile or scanned and sent via e-mail) shall be deemed original signatures. This Agreement does not create any partnership, joint venture or principal and agent relationship.

12.9 Hierarchy. The following order of precedence shall be applied in the event of conflict or inconsistency between provisions of the components of this Agreement: (i) the Software Order Form; (ii) the Schedules; (iii) the Use Terms; and (iv) the GTC.

Schedule B to the GTC
"Professional Services Schedule"

The parties agree that this Schedule is hereby annexed to and made a part of the GTC. In each instance in which provisions of this Schedule contradict or are inconsistent with the provisions of the GTC, the provisions of this Schedule shall prevail and govern.

WHEREAS, Licensee licensed from SAP the right to Use SAP Software pursuant to the Agreement and SAP provides, through its employees, affiliates, and third party contractors ("Consultants"), consulting and professional services ("Services") including support of installation and implementation of the licensed Software in the United States.

1. Services. Upon request by Licensee, SAP will provide a Consultant(s) to perform, at Licensee's direction, consulting and professional services including support of installation and implementation of the applicable SAP Software ("Services"). Any Statement(s) of Work ("SOW") more fully describing the project assumptions, scope, duration and fees for the Services shall reference this Schedule. All Services of the SAP Consultant(s) will be coordinated with the designated Licensee representative. Licensee is responsible for making the necessary internal arrangements for the carrying out of the Services on a non-interference basis.

2. Satisfaction with Performance. If at any time Licensee or SAP is dissatisfied with the material performance of an assigned Consultant or a Licensee project team member, the dissatisfied party shall immediately report such dissatisfaction to the other party in writing and may request a replacement. The other party shall use its reasonable discretion in accomplishing any such change.

3. Compensation of SAP. All Services will be provided by SAP on a time and expense basis at SAP's then current rates, unless otherwise agreed by the parties in a SOW.

4. Taxes. The fees listed in the applicable SOW do not include taxes. If SAP is required to pay sales, use, property, value-added or other taxes based on the Services provided under this Schedule, then such taxes shall be billed to and paid by Licensee. This section shall not apply to taxes based on SAP's income. Licensee also agrees to pay SAP for additional tax amounts if any, created by the taxability of Consultants reimbursed travel and living expenses resulting from long term assignments at Licensee's locations.

5. Work Product. Unless otherwise agreed to in writing by the parties in a SOW, SAP shall have the sole and exclusive right, title and ownership to any and all ideas, concepts, or other intellectual property rights related in any way to the techniques, knowledge or processes of the SAP Services and deliverables, whether or not developed for Licensee.

6. Warranty. SAP warrants that its Services shall be performed consistent with generally accepted industry standards. SAP MAKES NO WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, NOR ANY OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, IN CONNECTION WITH THIS SCHEDULE AND THE SERVICES PROVIDED HEREUNDER.

7. Limitation of Liability. WITH RESPECT TO SERVICES, ANYTHING TO THE CONTRARY NOTWITHSTANDING, EXCEPT FOR DAMAGES RESULTING FROM UNAUTHORIZED USE OR DISCLOSURE OF THE PROPRIETARY INFORMATION AND SAP'S RIGHT TO COLLECT UNPAID FEES, UNDER NO CIRCUMSTANCES SHALL SAP, ITS CONSULTANTS OR LICENSEE BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE SERVICES HEREUNDER OR BE LIABLE IN ANY AMOUNT FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES, LOSS OF GOOD WILL OR BUSINESS PROFITS, WORK STOPPAGE, DATA LOSS, COMPUTER FAILURE OR MALFUNCTION, OR EXEMPLARY OR PUNITIVE DAMAGES. The provisions of the Schedule allocate the risks between SAP and Licensee. The License Fees reflect this allocation of risk and the limitations of liability herein.

8. Termination. The terms of this Schedule shall be effective as of the Effective Date of the Agreement and shall remain in effect until terminated by either party upon thirty (30) days prior written notice or otherwise in accordance with a particular SOW. Licensee shall be liable for payment to SAP for all Services provided prior to the effective date of any such termination, including any expenses incurred pursuant to the provision of such Services, in accord with the applicable SOW.

9. General Provisions.
   9.1 SAP may subcontract all or part of the Services to be performed to a qualified third party.
   9.2 With respect to the Services provided by SAP under this Schedule and any SOW hereto, the relationship of SAP and Licensee is that of an independent contractor.
   9.3 This Schedule, including any applicable SOWs, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements between the parties, whether written or oral, relating to the same subject matter. In the event of any inconsistencies between this Schedule and a SOW, the SOW shall take precedence over the Schedule. Any purchase order or other document issued by Licensee is for administrative convenience only.

10. Survival. Sections 5 and 7 above shall survive any termination of this Schedule.

SUBSCRIPTION SERVICE AGREEMENT

This Subscription Service Agreement (including the Subscription Service Guide, attached hereto) ("***Agreement***") is made between the ServiceNow entity ("***ServiceNow***") and the customer entity ("***Customer***") on the ordering document and becomes effective on the last signature date of the ordering document issued by ServiceNow ("***Effective Date***").

The Subscription Service Guide includes: (1) the Customer Support Policy; (2) the Upgrade Policy; (3) the Data Security Guide; and (4) any other attachment set forth or referenced in the Subscription Service Guide. The Subscription Service Guide is posted on www.servicenow.com/schedules.do and incorporated herein by reference.

Pursuant to a separate transaction between Customer and ServiceNow's authorized reseller ("***Reseller***"), Customer has purchased from Reseller certain services to be delivered by ServiceNow. This Agreement specifies the terms and conditions under which those services will be provided, apart from price, payment and other terms specified in the separate agreement between Customer and Reseller.

1. DEFINITIONS

1.1. "***Confidential Information***" means: (a) ServiceNow Core Technology (which is Confidential Information of ServiceNow); (b) Customer Data and Customer Technology (which are Confidential Information of Customer); (c) any other information of a party that is disclosed in writing or orally and is designated as *Confidential* or *Proprietary* at the time of disclosure (and, in the case of oral disclosures, summarized in writing within thirty (30) days of the initial disclosure and delivered to the receiving party), or that due to the nature of the information the receiving party would clearly understand it to be confidential information of the disclosing party; and (d) the specific terms and conditions of this Agreement, any Use Authorization, any SOW, and any amendment and attachment thereof, between the parties. Confidential Information shall not include any information that: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving party; (ii) was rightfully in the receiving party's possession at the time of disclosure without restriction on use or disclosure; (iii) is independently developed by the receiving party without use of the disclosing party's Confidential Information; or (iv) was or is rightfully obtained by the receiving party from a third party not under a duty of confidentiality and without restriction on use or disclosure.

1.2. "***Customer Data***" means electronic data uploaded by or for Customer and Customer's agents, employees and contractors, and processed in the Subscription Service, excluding the ServiceNow Core Technology.

1.3. "***Customer Technology***" means software, methodologies, templates, business processes, documentation or other material authored, invented or otherwise created or licensed (other than by or from ServiceNow) by Customer using or for use with the Subscription Service, excluding the ServiceNow Core Technology.

1.4. "***Development Tools***" means source code, application programming interfaces (APIs), executable software and tools in human readable format made available by ServiceNow for the implementation, customization, configuration, and use of the Subscription Service, such as scripts, code snippets, sample code, and development tools published by ServiceNow.

1.5. "***Documentation***" means the ServiceNow product documentation relating to the operation and use of the Subscription Service, Software and Development Tools, including technical program or interface documentation, user manuals, operating instructions and release notes, as updated from time to time by ServiceNow.

1.6. "***Product Overview***" means the description of the ordered products and their functionalities attached to a Use Authorization or referenced therein.

1.7. "***Professional Services***" means any services provided by ServiceNow pursuant to an agreed SOW or Service Description.

1.8. "***Service Description***" means the written description for a packaged Professional Service, attached to a Use Authorization or referenced therein.

1.9. "***ServiceNow Core Technology***" means: (a) the Subscription Service; Software; Development Tools, Documentation; and ServiceNow technology and methodologies (including, without limitation, products, software tools, hardware designs, algorithms, templates, software (in source and object forms), architecture, class libraries, objects and documentation) existing as of the Effective Date or otherwise arising outside of work under a Professional Service; (b) updates, upgrades, improvements, configurations, extensions, and derivative works of the foregoing and related technical or end user documentation or manuals; and (c) intellectual property anywhere in the world relating to the foregoing.

1.10. "***Software***" means software provided by ServiceNow to Customer that operates on Customer-provided machines solely to facilitate the use of the Subscription Service.

1.11. "***SOW***" means a statement of work for Professional Services.

1.12. "***Subscription Service***" means the ServiceNow software as a service (SaaS) offering identified in a Use Authorization.

1.13. "***Subscription Term***" means the term of authorized use of the Subscription Service as set forth in the Use Authorization.

1.14. "***Use Authorization***" means a written document provided to Customer specifying the services that Customer has purchased, along with the term and scope of the authorized use thereof.

2. GRANT OF USE RIGHTS

2.1. SUBSCRIPTION SERVICE. Subject to the terms of this Agreement, ServiceNow authorizes Customer to access and use the purchased Subscription Service during the Subscription Term as set forth in an applicable Use Authorization for its internal business purposes in accordance with the Documentation. Customer shall not use or otherwise access the Subscription Service in a manner that exceeds Customer's authorized use as set forth in this Agreement and the applicable Use Authorization.

2.2. SOFTWARE. ServiceNow grants Customer a limited, personal, worldwide, non-sublicensable, non-transferable (except as set forth in Section 10.1 (Assignment)), non-exclusive license during the Subscription Term to install and execute Software on machines operated by or for Customer solely to facilitate Customer's authorized access to and use of the purchased Subscription Service. The Software may include code that is licensed under third party license agreements, including open source made available or provided with the Software. Software is licensed and not sold even if for convenience ServiceNow makes reference to words such as *sale* or *purchase*.

2.3. DEVELOPMENT TOOLS. In support of Customer's authorized internal business use of the Subscription Service during the Subscription Term, ServiceNow grants to Customer a limited, personal, worldwide, non-sublicensable, non-transferable (except as set forth in Section 10.1 (Assignment)), non-exclusive license to download and make a reasonable number of copies of the Development Tools, and to use, copy, modify and create derivative works of the Development Tools, in: (a) using, implementing and integrating the ServiceNow applications with other software and systems; and (b) creating applications on the ServiceNow platform (to the extent Customer has purchased authorized use of the Subscription Service to create applications on the ServiceNow platform). Customer shall not use the Development Tools in a manner that causes it to exceed the limits of its authorized use of the Subscription Service as set forth in this Agreement and the Use Authorization. From time to time, ServiceNow may provide Development Tools subject to the terms and conditions of separate agreements which will be provided to Customer for review and to which Customer will be required to agree prior to use of such Development Tools; provided that ServiceNow shall not require Customer to agree to separate terms and conditions for any Development Tool that is necessary for Customer's use of its ordered Subscription Service in conformance with the Product Overview unless set forth on the Use Authorization.

2.4. RESTRICTIONS. Customer shall not (and shall not permit others to) do the following with respect to the ServiceNow Core Technology: (i) use the Subscription Service with external programs in a manner that intentionally circumvents contractual usage restrictions; (ii) license, sub-license, sell, re-sell, rent, lease, transfer, distribute or time share or otherwise make any of it available for access by third parties except as otherwise expressly provided in a Use Authorization; (iii) access it for the purpose of developing or operating products or services intended to be offered to third parties in competition with the Subscription Service; (iv) disassemble, reverse engineer or decompile it; (v) copy, create derivative works based on or otherwise modify it except as permitted in this Agreement; (vi) remove or modify a copyright or other proprietary rights notice in it; (vii) use it to reproduce, distribute, display, transmit or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (viii) use it to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or otherwise engage in a malicious act or disrupt its security, integrity or operation; or (ix) access or disable any ServiceNow or third party data, software or network (other than Customer's instance of the Subscription Service in accordance with this Agreement). Before Customer exercises any of the foregoing actions that Customer believes it is entitled to, Customer shall provide ServiceNow with thirty (30) days' prior written notice to legalnotices@servicenow.com (or, if applicable law or the relevant court order does not allow for such notice, then the maximum amount of notice allowable), and provide reasonably requested information to allow ServiceNow to assess Customer's claim and, at ServiceNow's sole discretion, provide alternatives that reduce adverse impacts on ServiceNow's intellectual property and other rights.

3. ORDERING

3.1. RESELLER ORDERS. Customer shall order and purchase the Subscription Service and Professional Services directly from Reseller pursuant to a separate agreement specifying price, payment and other commercial terms. ServiceNow is not a party to such separate agreement but will provide the purchased services pursuant to this Agreement. For each order, Reseller or ServiceNow will provide Customer with a Use Authorization for Customer to sign and return to ServiceNow. ServiceNow will have no obligation to provide services unless and until it has received a Use Authorization signed by Customer. Reseller is not authorized to make any changes to this Agreement (including any Use Authorizations issued hereunder) or bind ServiceNow to any additional or different terms or conditions. Additional orders for ServiceNow products or services may be placed either through Reseller or ServiceNow, provided that if Customer places an order directly through ServiceNow, Customer shall sign an addendum to this Agreement setting forth pricing, payment and other commercial terms between Customer and ServiceNow.

3.2. USE VERIFICATION. ServiceNow or Reseller may remotely review Customer's use of the Subscription Service, and upon ServiceNow or Reseller's written request Customer shall provide any reasonable assistance, to verify Customer's compliance with the Agreement. If ServiceNow determines that Customer has exceeded its permitted use of the Subscription Service then ServiceNow will notify Customer and within thirty (30) days thereafter Customer shall either: (i) disable any unpermitted use or (ii) purchase additional subscriptions commensurate with Customer's actual use. If Customer fails to regain compliance within such thirty (30) day period or fails to make payment as provided in its agreement with Reseller, ServiceNow may suspend Customer's use of the Subscription Service or terminate this Agreement for cause in accordance with Section 9 (Term and Termination), in addition to any other rights or remedies ServiceNow may have.

4. INTELLECTUAL PROPERTY

4.1. SERVICENOW OWNERSHIP. As between ServiceNow and Customer, all rights, title, and interest in and to all intellectual property rights in the ServiceNow Core Technology are owned exclusively by ServiceNow notwithstanding any other provision in this Agreement. Except as expressly provided in this Agreement, ServiceNow reserves all rights in the ServiceNow Core Technology and does not grant Customer any rights, express or implied or by estoppel.

4.2. CUSTOMER OWNERSHIP. As between Customer and ServiceNow, Customer shall retain all of its rights, title, and interest in and to its intellectual property rights in Customer Data and Customer Technology. Customer hereby grants to ServiceNow a royalty-free, fully-paid, non-exclusive, non-transferable (except as set

forth in Section 10.1 (Assignment)), sub-licensable, worldwide right to use Customer Data and Customer Technology solely for the purpose of providing the Subscription Service and Professional Services to Customer.

4.3. FEEDBACK. ServiceNow encourages Customer to provide suggestions, proposals, ideas, recommendations or other feedback regarding improvements to ServiceNow's services and related resources. To the extent Customer provides such feedback, Customer grants to ServiceNow a royalty-free, fully paid, sub-licensable, transferable (notwithstanding Section 10.1 (Assignment)), non-exclusive, irrevocable, perpetual, worldwide right and license to make, use, sell, offer for sale, import and otherwise exploit feedback (including by incorporation of such feedback into the ServiceNow Core Technology) without restriction.

4.4. PROFESSIONAL SERVICES. Subject to the provisions of this Section 4.4, ServiceNow shall assign to Customer any Newly Created IP (as defined below) in Deliverables upon payment in full by Customer of all amounts due for the Professional Service under which the Deliverable was created. A "***Deliverable***" is a deliverable that is identified in the applicable SOW or Service Description and that is created by ServiceNow for Customer in the performance of the Professional Services. "***Newly Created IP***" means intellectual property in any inventions or works of authorship that are made by ServiceNow specifically for Customer in the course of performing Professional Services for Customer that is identified as "Newly Created IP" in an SOW, excluding the ServiceNow Core Technology. To the extent (if at all) any ServiceNow Core Technology is incorporated into a Deliverable, ServiceNow grants to Customer a non-exclusive, royalty-free, non-transferable, non-sublicensable worldwide license to use the ServiceNow Core Technology solely to use the Deliverable in connection with the Subscription Service as contemplated under this Agreement during the Subscription Term. Nothing in this Agreement shall be deemed to restrict or limit ServiceNow's right to perform similar Professional Services for any other party or to assign any employees or subcontractors to perform similar Professional Services for any other party or to use any information incidentally retained in the unaided memories of its employees providing Professional Services.

5. WARRANTIES

5.1. LIMITED SUBSCRIPTION SERVICE WARRANTY. ServiceNow warrants that during the Subscription Term Customer's production instances of the Subscription Service shall materially conform to the Product Overview. To submit a warranty claim under this Section, Customer shall (1) reference this Section; and (2) submit a support request to resolve the non-conformity as provided in the Subscription Service Guide. If the non-conformity persists without relief more than thirty (30) days after written notice of a warranty claim provided to ServiceNow under this Section 5.1, then Customer may terminate the affected Subscription Service and submit to Reseller a claim for refund of any prepaid subscription fees covering the remainder of the Subscription Term of the affected Subscription Service after the date of termination. Notwithstanding the foregoing, this warranty shall not apply to any non-conformity due to a modification of or defect in the Subscription Service that is made or caused by any person other than ServiceNow or a person acting at ServiceNow's direction. THIS SECTION 5.1 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

5.2. LIMITED PROFESSIONAL SERVICES WARRANTY. ServiceNow warrants that the Professional Services will be performed in a competent and workmanlike manner in accordance with accepted industry standards and practices and all material requirements set forth in the SOW or Service Description. Customer shall notify ServiceNow in writing of any breach within thirty (30) days after performance of the non-conforming Professional Services. Upon receipt of such notice, ServiceNow, at its option, shall either use commercially reasonable efforts to re-perform the Professional Services in conformance with these warranty requirements or shall terminate the affected Professional Services, in which case Customer may submit to Reseller a claim for a refund of any amounts paid for the nonconforming Professional Services. THIS SECTION 5.2 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

5.3. DISCLAIMER OF WARRANTIES. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED IN THIS AGREEMENT, TO THE MAXIMUM EXTENT ALLOWED BY LAW, SERVICENOW DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING WARRANTIES

ARISING UNDER STATUTE, WARRANTIES OF MERCHANTABILITY, ACCURACY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTIES ARISING FROM USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SERVICENOW SPECIFICALLY DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE, SOFTWARE, PROFESSIONAL SERVICES, DEVELOPMENT TOOLS, DOCUMENTATION OR DELIVERABLES WILL MEET THE REQUIREMENTS OF CUSTOMER OR OTHERS OR THAT THEY WILL BE ACCURATE OR OPERATE WITHOUT INTERRUPTION OR ERROR. CUSTOMER ACKNOWLEDGES THAT IN ENTERING THIS AGREEMENT IT HAS NOT RELIED ON ANY PROMISE, WARRANTY OR REPRESENTATION NOT EXPRESSLY SET FORTH HEREIN.

6. CONFIDENTIAL INFORMATION

6.1. CONFIDENTIALITY OBLIGATIONS. The recipient of Confidential Information shall: (i) at all times protect it from unauthorized disclosure with the same degree of care that it uses to protect its own confidential information, and in no event using less than reasonable care; and (ii) not use it except to the extent necessary to exercise rights or fulfill obligations under this Agreement. Each party shall limit the disclosure of the other party's Confidential Information to those of its employees and contractors with a need to access such Confidential Information for a party's exercise of its rights and obligations under this Agreement, provided that all such employees and contractors are subject to binding disclosure and use restrictions at least as protective as those set forth herein. Each party's obligations set forth in this Section 6 shall remain in effect during the term and three (3) years after termination of this Agreement. The receiving party shall, at the disclosing party's request or upon termination of this Agreement, return all originals, copies, reproductions and summaries of Confidential Information and other tangible materials and devices provided to the receiving party as Confidential Information, or at the disclosing party's option, certify destruction of the same. Provisions for the return of Customer Data are set forth in Section 9.3 (Return of Customer Data).

6.2. REQUIRED DISCLOSURES. A party may disclose the disclosing party's Confidential Information to a court or governmental body pursuant to a valid court order, law, subpoena or regulation, provided that the receiving party: (a) promptly notifies the disclosing party of such requirement as far in advance as possible to the extent advanced notice is lawful; and (b) provides reasonable assistance to the disclosing party in any lawful efforts by the disclosing party to resist or limit the disclosure of such Confidential Information.

6.3. EQUITABLE REMEDIES. The parties agree that the receiving party's disclosure of Confidential Information except as provided herein may result in irreparable injury for which a remedy in money damages may be inadequate. The parties further agree that in the event of such disclosure or threatened disclosure, the disclosing party may be entitled to seek an injunction to prevent the breach or threatened breach without the necessity of proving irreparable injury or the inadequacy of money damages, in addition to remedies otherwise available to the disclosing party at law or in equity.

7. INDEMNIFICATION

7.1. SERVICENOW OBLIGATION. Subject to the exclusions set forth below, ServiceNow shall: (i) defend Customer, its officers, directors and employees against any third party suit, claim, action or demand (each a *"**Claim**"*) to the extent alleging: (A) that the Subscription Service used in accordance with this Agreement infringes any third party patent, copyright or trademark, or misappropriates any third party trade secret; or (B) that ServiceNow's personnel when onsite at Customer's premises caused death, bodily harm or damage to tangible personal property due to their negligence or willful misconduct; and (ii) pay any court-ordered award of damages or settlement amount to the extent arising from any such Claims. If any portion of the Subscription Service becomes the subject of a Claim under Section 7.1(i)(A), ServiceNow may: (a) contest the Claim; (b) obtain permission from the claimant for Customer's continued use of the Subscription Service; (c) replace or modify the Subscription Service to avoid infringement, if such replacement or modification has substantially the same capabilities as the Subscription Service; or, if the foregoing (a), (b), and (c) are not available on commercially reasonable terms in ServiceNow's judgment, then (d) terminate Customer's use of the affected Subscription Service upon sixty (60) days' written notice, whereupon Customer may submit to Reseller a claim for a refund of any prepaid subscription fees covering the remaining portion of the applicable Subscription Term for the affected

Subscription Service after the date of termination. Notwithstanding the above, ServiceNow shall have no obligation or liability for any Claim under Section 7.1(i)(A) arising in whole or in part from: (1) any use of the Subscription Service which exceeds the authorized use permitted under this Agreement or not in accordance with the Documentation; (2) Customer Data or Customer Technology; (3) use of the Subscription Service by Customer in violation of applicable law; (4) use of the affected Subscription Service after termination in accordance with clause (d) of this Section 7.1; (5) modifications to the Subscription Service made to Customer's specifications or otherwise made by any person other than ServiceNow or a person acting at ServiceNow's direction if the Claim would have been avoided by use of the unmodified Subscription Service; or (6) use of the Subscription Service in combination with any hardware, software, application or service that was not provided by ServiceNow, if the Claim would have been avoided by the non-combined or independent use of the Subscription Service.

7.2. CUSTOMER OBLIGATION. Customer shall: (i) defend ServiceNow, its officers, directors and employees against any Claim alleging that: (A) Customer Data, (B) Customer Technology or (C) a modification to the Subscription Service made to Customer's specifications or otherwise made by or on behalf of Customer by any person other than ServiceNow or a person acting at ServiceNow's direction (but only if the Claim would have been avoided by use of the unmodified Subscription Service), infringes any patent, copyright or trademark, misappropriates any third party trade secret, or violates any third party privacy rights; and (ii) pay any court-ordered award of damages or settlement amount to the extent arising from such Claim.

7.3. PROCESS. All of the foregoing indemnity obligations of ServiceNow and Customer are conditioned on the indemnified party notifying the indemnifying party promptly in writing of any actual or threatened Claim, the indemnified party giving the indemnifying party sole control of the defense thereof and any related settlement negotiations, and the indemnified party cooperating and, at the indemnifying party's request and expense, assisting in such defense. SECTION 7 STATES EACH PARTY'S ENTIRE LIABILITY AND THE OTHER PARTY'S EXCLUSIVE REMEDY FOR THIRD PARTY CLAIMS AND ACTIONS.

8. LIMITATIONS OF LIABILITY

8.1. LIMITATIONS OF LIABILITY. SERVICENOW SHALL HAVE NO LIABILITY FOR ANY REFUND THAT, IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT, IS TO BE PAID BY RESELLER. TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCTS OR SERVICES PROVIDED HEREUNDER WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER FOR THE PRODUCTS OR SERVICES GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS LIMIT. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO:
(1) CUSTOMER'S OBLIGATION TO PAY FOR PRODUCTS, SERVICES OR TAXES; (2) A PARTY'S OBLIGATIONS IN SECTION 7 (INDEMNIFICATION); AND (3) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

8.2. EXCLUSION OF DAMAGES. TO THE EXTENT PERMITTED BY LAW, NEITHER SERVICENOW NOR CUSTOMER SHALL BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR LOST PROFITS (WHETHER DIRECT OR INDIRECT) OR LOSS OF USE OR DATA, COVER, SUBSTITUTE GOODS OR SERVICES, OR FOR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGE TO BUSINESS, REPUTATION OR GOODWILL), OR INDIRECT DAMAGES OF ANY TYPE HOWEVER CAUSED, WHETHER BY BREACH OF WARRANTY, BREACH OF CONTRACT, IN TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE CAUSE OF ACTION EVEN IF SUCH PARTY HAS BEEN ADVISED OF SUCH DAMAGES IN ADVANCE OR IF SUCH DAMAGES WERE FORESEEABLE. THE FOREGOING EXCLUSIONS SHALL NOT APPLY TO: (1) PAYMENTS TO A THIRD PARTY ARISING FROM A PARTY'S OBLIGATIONS UNDER SECTION 7 (INDEMNIFICATION); AND (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

8.3. GROSS NEGLIGENCE; WILFUL MISCONDUCT. AS PROVIDED BY LAW, NOTHING HEREIN SHALL BE INTENDED TO LIMIT A PARTY'S LIABILITY IN AN ACTION IN TORT (SEPARATE AND DISTINCT

FROM A CAUSE OF ACTION FOR BREACH OF THIS AGREEMENT) FOR THE PARTY'S GROSS NEGLIGENCE OR WILFUL MISCONDUCT.

9. TERM AND TERMINATION

9.1. TERM AND TERMINATION. This Agreement continues until terminated under the terms of this Agreement. Each party may terminate this Agreement in its entirety either: (i) upon thirty (30) days' prior written notice to the other party, if at the time of notice there are no Use Authorizations in effect; or (ii) upon written notice if the other party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership or liquidation, in any jurisdiction, that is not dismissed within sixty (60) days of its commencement or an assignment for the benefit of creditors. Either party may terminate a Subscription Service or Professional Services upon written notice if the other party materially breaches this Agreement or the applicable Use Authorization for the affected service and does not cure the breach within thirty (30) days after receiving written notice thereof from the non-breaching party. Professional Services are separately ordered from the Subscription Service, and are not required for the Subscription Service. A breach by a party of its obligations with respect to Professional Services shall not by itself constitute a breach by that party of its obligations with respect to the Subscription Service even if the services are enumerated in the same Use Authorization.

9.2. EFFECT OF TERMINATION OF SUBSCRIPTION SERVICE. Upon termination of the Subscription Service for any reason, Customer shall stop using, and ServiceNow shall stop providing, the Subscription Service and all rights granted to Customer in this Agreement shall terminate. If the Subscription Service is terminated by Customer due to ServiceNow's breach, then Customer may submit to Reseller a claim for refund of all prepaid fees for the remaining portion of the Subscription Term for the terminated Subscription Service after the effective date of termination. Within thirty (30) days following the effective date of a termination by ServiceNow for Customer's breach, Customer shall pay all remaining amounts for the Subscription Term applicable to the Subscription Service covering the remainder of the Subscription Term regardless of the due dates specified in Reseller's order form to Customer.

9.3. TRANSITION SERVICES. At least thirty (30) days prior to either the expiration of the Subscription Term (where Customer elects not to renew) or in connection with the termination by Customer of the Subscription Service in accordance with Section 9.1, provided that Customer signs an addendum to this Agreement setting forth payment and other commercial terms between Customer and ServiceNow, Customer may purchase the following services from ServiceNow: (i) one (1) extension of the Subscription Service for up to six (6) months ("***Transition Subscription Service***"); and (ii) Professional Services. Prior to the commencement of any Transition Subscription Service or Professional Services, Customer shall sign an ordering document and shall pay in advance for the Transition Subscription Service and any Professional Services plus verifiable travel and expenses.

9.4. RETURN OF CUSTOMER DATA. ServiceNow shall provide Customer Data in its standard database export format, excluding the ServiceNow Core Technology, to Customer upon Customer's written request and at no additional cost to Customer, provided that ServiceNow receives such request from Customer within forty-five (45) days following the expiration or termination of this Agreement for the Subscription Service (including any Transition Subscription Service term, if applicable).If ServiceNow has not received a request within the foregoing time frame, ServiceNow shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of the Subscription Service.

9.5. SURVIVAL. Sections 2.4 (Restrictions), 4.1 (ServiceNow Ownership), 4.2 (Customer Ownership), 4.3 (Feedback) and 6 (Confidential Information) through 10 (General Provisions) of this Agreement, together with any other provision required for their construction or enforcement, shall survive termination of this Agreement for any reason.

10. GENERAL PROVISIONS

10.1. ASSIGNMENT. Neither party may assign its rights or obligations under this Agreement, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the

foregoing, either party may, upon notice and without the other party's consent: (i) in connection with a merger, reorganization or sale of all or substantially all of the assets or equity of such party, assign this Agreement in its entirety to such party's successor; and (ii) assign this Agreement in its entirety to any Affiliate. "***Affiliates***" shall mean any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where "***Control***" means the legal power to direct or cause the direction of the general management of the company, partnership or other legal entity. Any attempted or purported assignment in violation of this Section 10.1 will be null and void. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

10.2. COMPLIANCE WITH LAWS. ServiceNow shall comply with any statutes and regulations that apply to its provision of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to the privacy and security of personal information, including trans-border data transfers and data breach notification requirements as required of ServiceNow by law. Customer shall comply with all laws that apply to its use of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to collection and processing of Customer Data in ServiceNow systems through the Subscription Service. Customer agrees to provide any required disclosures to and obtain any required consents for the transfer of Customer Data to ServiceNow. ServiceNow shall not be responsible for compliance with any laws applicable to Customer and its industry that are not generally applicable to information technology service providers.

10.3. EXPORT COMPLIANCE. Each party shall comply with United States and foreign export control laws and regulations. Customer acknowledges that the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables are subject to the U.S. Export Administration Regulations (the "***EAR***") and that Customer shall comply with the EAR. Without limiting the foregoing, Customer represents and warrants that: (i) Customer is not located in, and shall not use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables from, any country that is subject to U.S. export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan and Syria); (ii) Customer shall not use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, sounding rockets or unmanned air vehicle systems; and (iii) Customer is not prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. In addition, Customer is responsible for complying with any local laws which may impact Customer's right to import, export or use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables.

10.4. US GOVERNMENT RIGHTS. All ServiceNow software (including Software) is commercial computer software and all services are commercial items. "***Commercial computer software***" has the meaning set forth in Federal Acquisition Regulation ("***FAR***") 2.101 for civilian agency purchases and the Department of Defense ("***DOD***") FAR Supplement ("***DFARS***") 252.227-7014(a)(1) for defense agency purchases. If the software is licensed or the services are acquired by or on behalf of a civilian agency, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the services are acquired by or on behalf of any agency within the DOD, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses Government rights in computer software or technical data.

10.5. NOTICE. Except as otherwise provided herein, all notices shall be in writing and deemed given upon: (i) personal delivery; (ii) when received by the addressee if sent by a recognized overnight courier (receipt requested); (iii) the second business day after mailing; or (iv) the first business day after sending by email with

confirmation of receipt, except that email shall not be sufficient for notices regarding a Claim. Notices shall be sent to the parties as set forth on the signature page of this Agreement or as subsequently updated in writing.

10.6. FORCE MAJEURE. No party shall be liable or responsible to the other party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement (excluding Customer's failure to pay amounts owed when due), when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control, including without limitation: strikes, lock-outs or other industrial disputes (whether involving its own workforce or a third party's), trespassing, sabotage, theft or other criminal acts, failure of energy sources or transport network, acts of God, export bans, sanctions and other government actions, war, terrorism, riot, civil commotion, interference by civil or military authorities, national or international calamity, armed conflict, malicious damage, breakdown of plant or machinery, nuclear, chemical or biological contamination, explosions, collapse of building structures, fires, floods, storms, earthquakes, epidemics or similar events, natural disasters or extreme adverse weather conditions (each a "***Force Majeure Event***"). The party suffering a Force Majeure Event shall use reasonable efforts to mitigate against the effects of such Force Majeure Event.

10.7. HIGH RISK ACTIVITIES. Customer shall use the ServiceNow Core Technology within the intended business purposes described in the Documentation, and not for any purpose that requires fail-safe performance including, but not limited to, stock trading, financial transaction processing, management of hazardous facilities or applications for which failure could result in death, personal injury, or severe physical or environmental damage ("***High Risk Activity***"). ServiceNow, its licensors and suppliers expressly disclaim all warranties of fitness for any such use and Customer shall release and hold ServiceNow, its licensors and suppliers harmless from liability arising out of the use of the ServiceNow Core Technology for High Risk Activity.

10.8. USE OF AGGREGATE DATA. Customer agrees that ServiceNow may collect, use and disclose quantitative data derived from the use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes. All data collected, used, and disclosed will be in aggregate form only and will not identify Customer or its users.

10.9. ENTIRETY. This Agreement, together with the Use Authorizations, Product Overviews, SOWs, Service Descriptions, and the Subscription Service Guide (including the Customer Support Policy, the Upgrade Policy and the Data Security Guide), is the final and entire agreement between the parties regarding the products and services provided hereunder and supersedes all prior or contemporaneous oral or written agreements, representations, understandings, undertakings and negotiations with respect to the subject matter hereof. The terms of this Agreement apply to the exclusion of any other terms that Customer seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing. Customer acknowledges that it has not relied on any statement, promise or representation made or given by or on behalf of ServiceNow that is not set out in this Agreement. Customer's orders are not contingent on, and Customer has not relied on, the delivery of any future functionality regardless of any verbal or written communication about ServiceNow's future plans. This Agreement may be executed in counterparts, each of which shall be deemed to be an original.

10.10. WAIVER AND AMENDMENT. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of this Agreement must be in writing and signed by authorized representatives of both parties.

10.11. RELATIONSHIP OF THE PARTIES. The parties are independent contractors. Nothing in this Agreement shall be construed to create a partnership, joint venture or agency relationship. Neither party shall have any right or authority to assume or create any obligation of any kind expressed or implied in the name of or on behalf of the other party.

10.12. GOVERNING LAW; JURISDICTION AND VENUE. This Agreement shall be governed by the laws of the state of California, without regard to its conflict of laws principles. The parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Santa Clara County, California, for the purposes of adjudicating any dispute arising out of this Agreement. Each party hereto expressly consents to service of process by registered mail. To the extent permitted by law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods shall not apply.

Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's intellectual property rights.

10.13. CONSTRUCTION. Products and services shall be provided in the English language unless agreed otherwise. The parties confirm that they have requested that this Agreement and all related documents be drafted in English at the express wishes of the parties. Les parties confirment avoir expressément exigé que le présent contrat et les documents de ServiceNow qui y sont attachés soient rédigés en anglais. Section headings are for convenience only and are not to be used in interpreting this Agreement.

SUBSCRIPTION SERVICE GUIDE

Capitalized terms not defined herein shall have the meaning set forth in the ordering agreement or the use agreement between Customer and ServiceNow.

1. SUPPORT

During the Subscription Term, ServiceNow or its authorized reseller, as applicable, shall provide support for the Subscription Service as set forth in the ***Customer Support Policy*** attached hereto, and incorporated herein by reference.

2. UPGRADES

ServiceNow determines whether and when to develop, release and apply any Upgrade (as defined in the ***Upgrade Policy*** attached hereto, and incorporated herein by reference) to Customer's instances of the Subscription Service.

3. DATA SECURITY

ServiceNow shall implement and maintain security procedures and practices appropriate to information technology service providers to protect Customer Data from unauthorized access, destruction, use, modification, or disclosure, as described in the ***Data Security Guide*** attached hereto, and incorporated herein by reference.

4. INSURANCE

ServiceNow agrees to maintain in effect during the Subscription Term, at ServiceNow's expense, the following minimum insurance coverage:

(i) (a) Workers' Compensation Insurance, in accordance with applicable statutory, federal, and other legal requirements and (b) Employers' Liability Insurance covering ServiceNow's employees in an amount of not less than $1,000,000 for bodily injury by accident, $1,000,000 policy limit for bodily injury by disease, and $1,000,000 each employee for bodily injury by disease;

(ii) Commercial General Liability Insurance written on an occurrence form and including coverage for bodily injury, property damage, products and completed operations, personal injury, advertising injury arising out of the services and/or products provided by ServiceNow under this Agreement with minimum limits of $1,000,000 per occurrence/$2,000,000 aggregate;

(iii) Commercial Automobile Liability Insurance providing coverage for hired and non-owned automobiles used in connection with this Agreement in an amount of not less than $1,000,000 per accident combined single limit for bodily injury and property damage;

(iv) Combined Technology Errors' & Omission Policy with a $5,000,000 per Claim limit, including: (a) Professional Liability Insurance providing coverage for the services and software in this Agreement. Such coverage to be maintained for at least two (2) years after the termination of this Agreement; and (b) Privacy, Security, and Media Liability Insurance providing liability coverage for unauthorized access or disclosure, security breaches or system attacks, as well as infringements of copyright and trademark that might result from this Agreement; and

(v) Excess Liability over Employers' Liability, Commercial General Liability and Commercial Automobile Liability with a $5,000,000 aggregate limit.

For the purpose of this Section, a "***Claim***" means a written demand for money or a civil proceeding which is commenced by service of a complaint or similar pleading.

5. AVAILABILITY SERVICE LEVEL

5.1. DEFINITIONS

(a) "***Available***" means that the Subscription Service can be accessed by authorized users.

(b) "***Excused Downtime***" means: (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks.

(c) "***Maintenance Time***" means the time the Subscription Service is not Available due to service maintenance.

(d) "***Availability SLA***" means the percentage of total time during which Customer's production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime.

5.2. AVAILABLITY

If Customer's production instances of the Subscription Service fall below the Availability SLA of ninety-nine and eight-tenths percent (99.8%) during a calendar month, Customer's exclusive remedy for failure of the Subscription Service to meet the Availability SLAs is either: (1) to request that the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or (2) to request that ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per minute rate ServiceNow charges to Customer for Customer's use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees.

5.3. REQUESTS

Customer must request all service credits or extensions in writing to ServiceNow within thirty (30) days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer's production instances of the Subscription Service was not Available. The total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for the month, and has no cash value. ServiceNow may delay issuing service credits until such amounts reach one thousand U.S. dollars ($1,000) or equivalent currency specified in the applicable Order Form.

CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that ServiceNow or its authorized reseller, as applicable, will provide for the Subscription Service. This Policy may be updated from time to time.

Scope

The purpose of Customer Support is to resolve defects that cause the Subscription Service to perform not in substantial conformance to the Product Overview. A resolution to a defect may consist of a fix, workaround or other relief ServiceNow deems reasonable.

Customer Support does not include:

- implementation services
- configuration services
- integration services
- customization services or other custom software development
- training
- assistance with administrative functions

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of the Subscription Service made by any person other than ServiceNow or a person acting at ServiceNow's direction.

Business Hours

Customer Support is available 24 hours a day, 7 days a week, including all holidays.

Access Contacts

Customer may contact ServiceNow using one of the following means:

- Support Portal at https://hi.service-now.com/. Customer may get login access to this self-service portal by contacting its ServiceNow administrator.
- Phone using one of the numbers at http://servicenow.com/support/contact-support.html.

Customer shall contact ServiceNow's authorized reseller in accordance with its agreement with the reseller.

Incident Priority

Incident priority for a defect is determined using the guidelines below:

Priority	Definition
P1	Any defect that causes an instance to be unavailable.
P2	Any defect that causes a critical function to fail.
P3	Any defect that significantly impedes work or progress.
P4	Any defect that does not significantly impede work or progress.

Response Times and Level of Effort

Customer submits an incident with ServiceNow via phone or web and with ServiceNow's authorized reseller as directed by reseller. All support requests are tracked online and can be viewed by Customer's authorized contacts. Response times do not vary if the incident was filed via phone or web.

ServiceNow or its authorized reseller, as applicable, will use reasonable efforts to meet the target response times and target level of effort stated in the table below. Support from the reseller may be limited to business hours only.

Priority	Target Response Times	Target Level of Effort
P1	30 minutes	Continuously, 24 hours per day, 7 days per week
P2	2 hours	Continuously, but not necessarily 24 hours per day, 7 days per week
P3	1 business day	As appropriate during normal business hours
P4	N/A	Varies

Customer Responsibilities

Customer's obligations are as follows:

(a) Customer agrees to receive from ServiceNow or its authorized reseller, as applicable, communications via email, phone or through the Support Portal regarding the Subscription Service.

(b) Customer shall appoint no more than five (5) contacts ("***Customer Authorized Contacts***") to engage Customer Support for questions and/or technical issues.

(i) Only Customer Authorized Contacts are authorized to contact Customer Support.

(ii) Customer must ensure the information for these contacts is current in the Support Portal at https://hi.service-now.com/.

(iii) Customer Authorized Contacts are trained on the use and administration of the Subscription Service.

(c) Customer shall cooperate to enable ServiceNow to deliver the Subscription Service and support for the service.

(d) Customer is solely responsible for the use of the Subscription Service by its authorized users.

Support Resources

- ServiceNow Website (http://www.servicenow.com/services/overview.html)
- ServiceNow Community (https://community.servicenow.com/welcome)
- Release Notes (http://wiki.service-now.com/index.php?title=Main_Page)
- Product Documentation (http://wiki.service-now.com/index.php?title=Main_Page)
- Knowledge Base (https://hi.service-now.com/nav_to.do?uri=kb_home.do)
- Support Community (https://community.servicenow.com/community/support)

UPGRADE POLICY

1. UPGRADES

"***Upgrades***" are ServiceNow's releases of the Subscription Service for repairs, enhancements or new features applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term. ServiceNow has the discretion to provide new functionality as an Upgrade or as different software or service for a separate fee. ServiceNow determines whether and when to develop, release and apply any Upgrade to Customer's instances of the Subscription Service.

2. NOTICE; MAINTENANCE DOWNTIME

ServiceNow shall use reasonable efforts to give Customer thirty (30) days prior notice of any Upgrade to the Subscription Service. ServiceNow shall use reasonable efforts to give Customer ten (10) days prior notice of any Upgrade to the cloud infrastructure network, hardware, or software used by ServiceNow to operate and deliver the Subscription Service if ServiceNow in its reasonable judgment believes that the infrastructure Upgrade will impact Customer's use of its production instances of the Subscription Service. ServiceNow will use commercially reasonable efforts to limit the period of time during which the Subscription Service is unavailable due to the application of Upgrades to no more than two (2) hours per month. Notwithstanding the foregoing, ServiceNow may provide Customer with a shorter or no notice period of an Upgrade if necessary, in the reasonable judgment of ServiceNow, to maintain the availability, security or performance of the Subscription Service or the ability of ServiceNow to efficiently provide the Subscription Service.

3. NOMENCLATURE

A pending Upgrade may be a "Feature Release", "Patch" or "Hotfix." A "***Feature Release***" is an Upgrade that includes new features or enhancements. A "***Patch***" or a "***Hotfix***" is an Upgrade to a Feature Release that maintains the functionality of the Feature Release and does not include new functionality. ServiceNow refers to each Feature Release and its associated Patches and Hotfixes as a "***Release Family***." For example, ServiceNow's Feature Release "Aspen" established the "Aspen" Release Family, and ServiceNow's subsequent Feature Release "Berlin" established the "Berlin" Release Family.

4. PINNING REQUESTS

Customer may submit a support request for "no Upgrade" not fewer than five (5) business days' prior to a pending Upgrade of the Subscription Service. Subject to the terms and conditions of this Upgrade Policy, Customer's "no Upgrade" request shall be granted, and the Upgrade shall not be applied to Customer's instances of the Subscription Service.

5. SUPPORTED AND NON-SUPPORTED RELEASE FAMILIES

ServiceNow offers support for the then current Release Family and the prior two (2) Release Families ("***Supported Release Families***") as set forth in the Customer Support Policy. A Customer using a Supported Release Family may be required to Upgrade to a Patch or Hotfix within the Supported Release Family to correct a defect. At its discretion, ServiceNow may offer limited support for additional Release Families ("***Non-Supported Release Families***"). Without limiting ServiceNow's discretion to determine the availability of support for Non-Supported Release Families, a Customer using a Non-Supported Release Family may be required to Upgrade to a Supported Release Family to correct a defect. Any service level agreements, recovery time objectives or recovery point objectives are not applicable to Non-Supported Release Families. Details of ServiceNow support are further set forth in the Customer Support Policy.

Customer acknowledges that the current Release Family is the most current feature, availability, performance and security version of the Subscription Service. Within a Supported Release Family, the most recent Patch contains the most current feature, availability, performance and security version of the Subscription Service for that Release Family. A Customer that has submitted a "no Upgrade" request may experience defects, for which Customer hereby agrees that ServiceNow is not responsible, including without limitation those that affect the features, availability, performance and security of the Subscription Service, that are fixed in the most

current version of the Subscription Service.

6. REQUIRED UPGRADES

If Customer has requested "no Upgrade" it may nevertheless be required to Upgrade if in the reasonable judgment of ServiceNow the Upgrade is necessary to maintain the availability, security or performance of the Subscription Service or the ability of ServiceNow to efficiently provide the Subscription Service, as follows:

6.1. SUPPORTED RELEASE FAMILY. If Customer is using a Supported Release Family, it may be required to Upgrade to a Patch or Hotfix within the Supported Release Family.

6.2. NON-SUPPORTED RELEASE FAMILY. If Customer is using a Non-Supported Release Family, it may be required to Upgrade to a Supported Release Family.

7. EXCEPTIONS

Notwithstanding the other provisions of this Upgrade Policy, Customer may not submit a support request for "no Upgrade" for any Upgrade to, or that is essential for, the infrastructure network, hardware, or software used by ServiceNow to operate and deliver the Subscription Service.

DATA SECURITY GUIDE

Security Statement of an Enterprise IT Cloud Company

The ServiceNow cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability and security. ServiceNow's comprehensive approach to address this demand is enabled by the following: (a) ServiceNow's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery; (b) ServiceNow achieves flexibility and control in its ability to deliver a stable user experience to the customer by having a logical single tenant architecture; (c) ServiceNow's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering those applications in a reliable and secure cloud environment; (d) ServiceNow invests in a comprehensive compliance strategy that allows its customers to attain their own compliance to applicable laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and (e) ServiceNow's homogeneous environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible.

This Data Security Guide describes the measures ServiceNow takes to protect Customer Data when it resides in the ServiceNow cloud. This Data Security Guide forms a part of any legal agreement into which this Data Security Guide is explicitly incorporated by reference (the "***Agreement***") and is subject to the terms and conditions of the Agreement. Capitalized terms that are not otherwise defined herein shall have the meaning given to them in the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow shall maintain a written information security program of policies, procedures and controls ("***Security Program***") governing the processing, storage, transmission and security of Customer Data. The Security Program includes industry standard practices designed to protect Customer Data from unauthorized access, acquisition, use, disclosure, or destruction. ServiceNow may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that any such update does not materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. CERTIFICATIONS AND ATTESTATIONS

2.1. Certifications and Attestations. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001 and SSAE 16 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "***Standards***") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall perform an assessment against such Standards ("***Assessment***"). Upon Customer's written request, which shall be no more than once per calendar year, ServiceNow shall provide a summary of the Assessment(s) to Customer. Assessments shall be Confidential Information of ServiceNow.

2.2. Safe Harbor. ServiceNow shall maintain self-certified compliance under the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks developed by the U.S. Department of Commerce regarding the collection, use and retention of Personal Data (defined in Section 6 below) from European Union member countries and Switzerland.

3. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

The Security Program shall include the following physical, technical and administrative measures designed to protect Customer Data from unauthorized access, acquisition, use, disclosure, or destruction:

3.1. Physical Security Measures

(a) Data Center Facilities: (i) Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (for example,

fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (ii) fire detection and fire suppression systems both localized and throughout the data center floor.

(b) Systems, Machines and Devices: (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

(c) Media: (i) Industry standard destruction of sensitive materials before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Customer Data.

3.2. Technical Security Measures

(a) Access Administration. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production systems. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationship. Production infrastructure includes appropriate user account and password controls (for example, the required use of virtual private network connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

(b) Logging and Monitoring. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

(c) Firewall System. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.

(d) Vulnerability Management. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

(e) Antivirus. ServiceNow updates anti-virus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

(f) Change Control. ServiceNow ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

3.3. Administrative Security Measures

(a) Data Center Inspections. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.

(b) Personnel Security. ServiceNow performs background and drug screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then current applicable standard operating procedure and subject to applicable law.

(c) Security Awareness and Training. ServiceNow maintains a security awareness program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.

(d) Vendor Risk Management. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

4. DATA PROTECTION AND SERVICE CONTINUITY

4.1. Data Centers; Data Backup. ServiceNow shall host Customer's instances in primary and secondary SSAE 16 Type II or ISO 27001 certified (or equivalent) data centers in the geographic regions specified on the Order Form for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.

4.2. Personnel. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a ServiceNow telephone support representative, geographically located to ensure business continuity for support operations.

5. INCIDENT MANAGEMENT AND BREACH NOTIFICATION

5.1. Incident Monitoring and Management. ServiceNow shall monitor, analyze and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. Depending on the nature of the incident, ServiceNow security group will escalate and engage response teams necessary to address an incident.

5.2. Breach Notification. Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow shall report to Customer the unauthorized acquisition, access, use, disclosure or destruction of Customer Data (a "Breach") promptly following determination by ServiceNow that a Breach occurred. The initial report shall be made to Customer security contact(s) designated in ServiceNow's customer support portal. ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted Data Subjects (defined in 6.1 below) and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach.

5.3. Customer Cooperation. Customer agrees to cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, identify its root cause(s) and prevent a recurrence.

6. DATA PROCESSING GUIDELINES; COMPLIANCE WITH LAWS

6.1. Customer as Data Controller. Customer acknowledges that in relation to Personal Data supplied and/or processed under the Agreement it acts as Controller and it warrants that it will duly observe all of its obligations under all applicable laws and regulations of the European Union, the European Economic Area and their member states regarding the processing of Personal Data (collectively referred to as "Data Protection Laws") including, without limitation, obtaining and maintaining all necessary notifications and obtaining and maintaining all necessary Data Subject Consents. Customer shall (i) have sole responsibility for the accuracy, quality, integrity, legality and reliability of Personal Data and of the means by which it acquired Personal Data, (ii) ensure that data processing instructions given to ServiceNow comply with applicable Data Protection Laws, and (iii) comply with all applicable Data Protection Laws in collecting, compiling, storing, accessing and using Personal Data in connection with the Subscription Service. For the purposes of this Data Security Guide, "Personal Data", "Controller", "Data Subject" and "Data Subject Consent" shall have the meaning given to these terms in Directive 95/46/EC. For clarity, "process" or "processing" means any operation or set of operations performed upon Customer Data.

6.2. ServiceNow as Data Processor. ServiceNow shall process or otherwise use Personal Data (including possible onward transfers) on behalf of Customer solely for the purpose of providing the services

described in the Agreement and only in accordance with Customer's lawful instructions (limited to those instructions which ServiceNow can reasonably carry out in the provision of the Subscription Service), the terms of the Agreement, and this Data Security Guide. ServiceNow shall ensure that those employees to whom it grants access to such Personal Data are directed to keep such Personal Data confidential and are informed of any additional data protection obligations applicable to such Personal Data. ServiceNow shall, to the extent legally permitted, promptly notify Customer with respect to any request or communication ServiceNow receives from any regulatory authority in relation to any data processing activities ServiceNow conducts on behalf of Customer. In addition, ServiceNow will cooperate and assist Customer, at Customer's cost, in relation to any such request and to any response to any such communication. ServiceNow will pass on to the Customer any requests of a Data Subject to access, delete, correct, or block Personal Data processed under the Agreement. If ServiceNow is compelled by law to disclose Customer's information as part of a civil proceeding to which Customer is a party, and Customer is not contesting the disclosure, Customer will reimburse ServiceNow for its reasonable cost of compiling and providing secure access to that information.

6.3. Subcontractors. ServiceNow may engage subcontractors for processing Customer Data under the Agreement, provided ServiceNow shall ensure compliance by such subcontractor(s) with the requirements of this Section 6 by entering into written agreements with such subcontractors which provide that the subcontractor will apply the Safe Harbor principles to the processing of Personal Data. ServiceNow's use of any subcontractor will not relieve, waive or diminish any obligation ServiceNow has under the Agreement or this Data Security Guide.

7. PENETRATION TESTS

7.1. By a Third Party. ServiceNow contracts with third party vendors to perform an annual penetration test on the ServiceNow platform to identify risks and remediation that help increase security.

7.2. By Customer. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of its instances of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request using ServiceNow's online support portal and completing a penetration testing agreement. ServiceNow and Customer must agree upon a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, and must not interfere with ServiceNow's day-to-day operations. Promptly upon completion of the penetration test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the test results as Confidential Information of ServiceNow.

8. SHARING THE SECURITY RESPONSIBILITY

8.1. Product Capabilities. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service.

8.2. Customer Responsibilities. ServiceNow provides the cloud environment that permits Customer to use and process Customer Data in the Subscription Service. The architecture in the Subscription Service includes, without limitation, column level encryption functionality and the access control list engine. Customer shall be responsible for using the column level encryption functionality and access control list engine for protecting all Customer Data containing sensitive data, including without limitation, credit card numbers, social security numbers, financial and health information, and sensitive personal data. Customer is solely responsible for the results of its decision not to encrypt such sensitive data. ServiceNow protects all Customer Data in the ServiceNow cloud infrastructure equally in accordance with this Data Security Guide, regardless of the classification of the type of Customer Data. Customer shall be responsible for protecting the confidentiality of each user's login and password and shall manage each user's access to the Subscription Service.

8.3. Customer Cooperation. Customer shall promptly apply any application upgrade that ServiceNow determines is necessary to maintain the security, performance or availability of the Subscription Service.

8.4. Limitations. Notwithstanding anything to the contrary in the Agreement or this Data Security Guide, ServiceNow's obligations extend only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. This Data Security Guide does not apply to: (i) information shared with ServiceNow that is not data stored in its systems using the Subscription Service; (ii) data in Customer's virtual private network (VPN) or a third party network; or (iii) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide.

ServiceNow Product Overview

Effective Date: May 2, 2016

ServiceNow Applications	
Activity Designer	Enables a user to construct reusable activities that suit an organization's business needs. Requires Orchestration Core.
Activity Packs	A collection of related workflow activities that allow Orchestration Core to connect to, and automate work with, external systems. Some Activity Packs require Orchestration Core and others require Cloud Management.
Agile Development	Provides capabilities to manage the software development process in projects including enhancement requests, defect prioritization, definition of release content, and tasks.
Asset Management	Provides capabilities to track and manage the physical, contractual, and financial aspects of assets.
Audit Management	Provides a centralized process for Internal Audit teams to automate the complete audit lifecycle by providing the capability to plan, scope and execute integrated, risk-based audit plans.
Change Management	Allows repeatable methods and procedures to be used for introducing change into the IT infrastructure by providing capabilities for creating, assessing, approving, and executing changes.
Client Software Distribution	Allows administrators to distribute software from the service catalog using third party management systems. Requires Orchestration Core.
Cloud Management	Provides the capability to automate the provisioning and management lifecycle of public and private virtual servers. Requires Orchestration Core.
Configuration Automation	Provides the capability to manage the configuration settings of a physical or virtual server. Requires Orchestration Core.
Cost Management	Provides capabilities to track one-time and recurring costs of configuration items used by IT and allocate those costs to business units using allocation rules.
Cost Transparency	Provides insight for executives seeking to align spending to business goals. Users can classify general ledger records, define reporting structures and allocation rules, and view summary reports.
Customer Service Management	Includes the following key features: Omni–channel customer engagement across portal, chat, email, and phone (native telephony integration requires Notify); a robust customer data model for accounts, partners, and contacts; case management with advanced skills-based routing, real-time service level agreement (SLA), service contracts and service entitlements; pre-packaged service analytics using both real-time data as well as snapshots for trend analysis (trend analytics requires Performance Analytics use rights); and voice of customer feedback through online surveys and customer satisfaction reporting.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.

ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Demand Management	Consolidates IT requests through a service catalog and routes them in a workflow to stakeholders who gather additional information to prioritize investment decisions.
Discovery	Locates physical and virtual devices connected to an enterprise network. When Discovery locates a device, it explores its configuration, status, software, and relationships to other connected devices, and updates the Configuration Management Data Base (CMDB).
Edge Encryption	Resides on Customer-owned servers and encrypts and decrypts eligible data stored in their instance. Customer controls and manages the encryption keys for the eligible data in their instance.
Enterprise Service Portal - HR	In support of HR service delivery, provides employee self-service via an HR service catalog and provides HR the capability to assign tasks to employees. Uses prebuilt layouts, controls, and content. Requires HR Service Management.
Event Management	Aggregates events from monitoring tools used by Customer in its infrastructure, de-duplicates and correlates inputs from such events to CMDB, and provides the ability to filter and prioritize events to create incidents for remediation.
Facilities Service Management	Provides capabilities to manage the service delivery of a facilities department by offering a self-service catalog and assignment of requests based on fulfillment rules.
Field Service Management	Provides capabilities to create work order records for the repair and service of equipment. Requires Asset Management.
Financial Planning	Assists executives and budget owners in the automation of budget and forecast planning, helping to increase efficiency and simplify the planning process.
Finance Service Management	Enables the finance department to define its services and fulfill requests through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
HR Service Management	Provides capabilities to manage HR service delivery using case management to document the interactions between the employee and HR supported by the knowledge base.
Incident Management	Facilitates the process of restoring normal IT operations by providing capabilities to record, classify, distribute, and manage incidents through to resolution. Includes Performance Analytics limited to 15 key performance indicators (KPIs), one dashboard and 90 days of data captured by Incident Management.
Legal Service Management	Enables the legal department to define its services and fulfill requests through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
Marketing Service	Enables the marketing department to define its services and fulfill requests

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Management	through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
Notify	Provides the capability to initiate notification from Customer's instance of the subscription service to a supported third-party platform for SMS, voice and other communications protocols. Customer is required to separately purchase any third-party service required to work with Notify.
Orchestration Core	Enables orchestration of activities outside Customer's instance of the subscription service. Allows Customer to automate discrete tasks or processes using graphical workflows that interact with external systems or services.
Password Reset	Provides the capability to reset User's passwords that are stored and pre-authenticated in a credential store outside Customer's instance of the subscription service, such as Active Directory and other supported credential stores. Requires Orchestration Core.
Performance Analytics	Provides advanced analytics and time series analysis for KPIs.
Platform Runtime	Allows customer to deploy applications developed on the ServiceNow Platform into production.
Policy and Compliance Management	Provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and best practices. Additionally, the application provides structured workflows for the identification, assessment, and continuous monitoring of control activities.
Problem Management	Facilitates the process of identifying the root causes of errors in the IT infrastructure by providing capabilities to record, escalate, and manage problems through to resolution.
Project Portfolio Management	Provides capabilities to plan, organize, and manage projects and project portfolios including associated tasks and resources.
Release Management	Facilitates the planning, design, build, configuration, testing, and release of hardware and software into the IT infrastructure.
Request Management	Provides capabilities to approve and fulfill requests for goods and services defined and presented in the service catalog.
Resource Management	Provides a view of projects and the availability, allocation, and capacity of assigned resources.
Risk Management	Provides an executive view into risk to allow risk managers to quickly identify at-risk assets, perform assessments, and continuously monitor risk exposure.
Security Incident Response	Enables SOC/SIRT teams to enact response plans to address security-related activities, events or incidents. Enables response team collaboration, investigation of network and non-network related activities (i.e. intellectual property theft, criminal activities, etc.) and includes the capability for automated request assignment and remediation across IT and security teams.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.

ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Service Mapping	Discovers business services of the organization and builds a comprehensive map of all devices, applications, and configuration profiles used in these business services.
Test Management	Provides a user acceptance testing framework to help project teams and business users align on project deliverables, and provides visibility into the status of the project testing when used in conjunction with Project Portfolio Management and Agile Development. Project Portfolio Management and Agile Development are separately authorized.
Threat Intelligence	Provides the ability to support multiple threat intelligence feeds to enhance the context of a security incident by enabling analysts to see potential threats and related systems in an integrated view. Threat Intelligence also allows Customers to add their own custom feeds and to place confidence scores or weighting on each feed to accelerate the identification of legitimate security issues.
Vendor Performance Management	Enables Customer to manage, evaluate and compare vendors based on predefined criteria.
Vulnerability Response	Integrates with the National Vulnerability Database (NVD) and third-party solutions to generate a set of actionable reports of vulnerable assets in the Customer environment. Incident response tasks, change requests or problem tickets can easily be opened from vulnerabilities to allow security teams to perform further investigation or to allow IT to perform remediation.
ServiceNow Platform Services	
Business Service Maps	Graphically displays the configuration items related to a business service, and indicates the status of those configuration items.
Chat	Provides real-time communication capability via instant messaging between Users.
Coaching Loops	Provides the capability to monitor and provide feedback on a specific behavior of an individual or group.
Configuration Management (CMDB)	Provides capabilities to identify, record, and report on IT configuration items and their relationships.
Connect	Provides the capability to connect people, processes and information into a unique and centralized collaboration workspace to cut down on resolution times. Features include real-time chat, document delivery, active lists to see who is working and the ability to interact straight from the activity stream.
Content Management System	Provides the ability to create custom interfaces.
Form Designer	Allows creation of forms and tables with visual controls.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Google Maps	ServiceNow may make Google Maps available for use with the subscription service. If Customer uses Google Maps, Customer agrees to the following terms: (i) Customer shall limit its use to 60,000 map views on an annual basis and additional use shall be purchased from Google subject to Google's terms and conditions, to which ServiceNow is not a party; (ii) Customer agrees, and shall cause its end users to agree, to Google's Maps Terms (http://maps.google.com/help/terms_maps.html or a successor URL as provided by Google), the Legal Notices (http://www.maps.google.com/help/legalnotices_maps.html or a successor URL as provided by Google), and the Acceptable Use Policy (http://www.google.com/enterprise/earthmaps/legal/us/maps_AUP.html or a successor URL as provided by Google); and (iii) Customer agrees that Google may use Customer data in accordance with its privacy policy and that Google may provide its maps services to Customer. Google Maps may not be available to Customer due to location availability and may not be available during Customer's entire subscription term. ServiceNow support and warranty do not apply to Google Maps.
Graphical Workflow	Provides the capability to automate multi-step processes within Customer's instance of the subscription service. Each workflow can manage a sequence of activities, such as creating records or running scripts, and the condition-based transitions between them. Customer is required to purchase Orchestration Core to orchestrate activities using the Graphical Workflow that interact outside Customer's instance of the subscription service.
Knowledge Management	Provides role-based tools to create, store, and publish information. Provides mechanisms for version control and approvals of documents in the review process.
Live Feed	Provides a place to post and share content.
Mobile	Provides a customizable ServiceNow interface for mobile devices.
On-Call Scheduling	Enables creation of on-call schedules and escalation rosters.
OpenFrame	An interface technology that enables real-time communication channels such as telephone systems to be integrated into the ServiceNow Platform. OpenFrame consists of UI elements as well as a set of APIs that support exchange of events and data between ServiceNow and the communications system.
Reporting	Provides the capability to create and share reports and dashboards.
REST API	Provides the ability to integrate external systems through REST APIs using standard respond codes, header information, pagination support and streaming data on requests.
Service Catalog	Displays a listing of the goods and services that Customer provides within the enterprise to its employees and contractors.
Service Creator	Provides capabilities for building no-code service catalog items.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Service Level Management	Establishes and monitors status of service contracts and SLAs between the organization and its customers or third-party service providers.
Service Portal Designer	Provides the capability to build portals with a consumer-like experience using both ServiceNow out-of-the-box widgets and templates as well as Customer's own widgets and styles, while leveraging only HTML and CSS.
Skills Management	Assigns configured competencies to groups or users.
Studio	Integrated Development Environment (IDE) for professional and low-code (i.e., IT administration) application developers.
Survey Management	Allows for polling and collection of data, including configuration for specific events and/or conditions.
Time Cards	Records time worked on tasks either manually or automatically.
Visual Task Boards	Enables a Kanban-style workspace for either individual or team-based management of tasks.
Visualizations	Displays interactive 2-D and 3-D visual representations for any logical data relationships within an instance.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.

ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

GENERAL TERMS AND CONDITIONS

These General Terms and Conditions and any referenced documents form the agreement (the "***Agreement***") under which an Order Form is executed.

1. PROVISION OF SERVICES

ServiceNow will make the following purchased services available to Customer, subject to the terms and conditions of the Agreement and each ordering document signed by Customer and ServiceNow (each, an "***Order Form***") and the product overview attached thereto or referenced therein ("***Product Overview***"), including without limitation:

(a) use of the ServiceNow applications which are made available by ServiceNow as a software as a service (SaaS) ("***Subscription Service***"); and

(b) professional services and training services ("***Professional Services***").

An Order Form for Professional Services shall specify ServiceNow packaged professional services (each offering, a "***Packaged Service***"), as described in one or more service descriptions (if not attached to the Order Form, then as set forth on www.servicenow.com/be_schedules.do) ("***Service Description***") or other Professional Services described in one or more written statements of work ("***SOW***") signed by ServiceNow and Customer.

2. ORDERING

2.1 ORDERS AND PAYMENT. Upon execution by Customer and ServiceNow, each Order Form is non-cancellable and non-refundable except as provided in the Agreement. Prices stated in each Order Form are final. Except as expressly set forth in the applicable Order Form, Subscription Service fees are invoiced annually in advance. Each Subscription Term (as defined in Section 3.1) as set forth in the Order Form is a continuous and non-divisible commitment for the full duration of the Subscription Term regardless of the invoice schedule. Except as expressly set forth in the applicable Order Form or SOW or Service Description, Professional Services fees are invoiced on a time and materials basis monthly in arrears. Customer shall pay each invoice in full within thirty (30) days after the date of invoice. Customer may issue a purchase order consistent with the terms of the Order Form, but a purchase order is not required. If Customer issues a purchase order, then it shall be for the full amount of the Order Form, and any additional or conflicting terms appearing in a purchase order shall not amend the Order Form or the Agreement. Upon request, ServiceNow shall reference the purchase order number on its invoices (solely for administrative convenience) so long as Customer provides the purchase order at least fifteen (15) business days prior to the date of the invoice. Late payments shall accrue interest at a rate of one and one-half percent (1.5%) per month or the legal maximum interest rate, whichever is lower. If Customer is delinquent in payment of amounts for the services owed hereunder, ServiceNow may give notice to Customer of such delinquency and, in such case, Customer shall cure the delinquency within thirty (30) days from the date of ServiceNow's written notice. If Customer fails to cure the delinquency, ServiceNow may suspend Customer's use of the Subscription Service or terminate the Agreement for cause in accordance with Section 7 (Term and Termination), in addition to other rights and remedies available.

2.2 TAXES. All payments required by the Agreement are stated exclusive of all taxes, duties, levies, imposts, fines or similar governmental assessments including sales and use taxes, value-added taxes ("***VAT***"), goods and services taxes ("***GST***"), excise, business, service, and similar transactional taxes imposed by any jurisdiction and the interest and penalties thereon (collectively, "***Taxes***"). Customer shall be responsible for and bear Taxes associated with its purchase of, payment for, access to or use of the Subscription Service and Professional Services. Taxes shall not be deducted from the payments to ServiceNow, except as required by law, in which case Customer shall increase the amount payable as necessary so that after making all required deductions and withholdings, ServiceNow receives and retains (free from any Tax liability) an amount equal to the amount it would have received had no such deductions or withholdings been made. Each party is responsible for and shall bear taxes imposed on its net income. If Customer is a tax-exempt entity or claims exemption from any Taxes under the Agreement, Customer shall provide a tax exemption number on the Order Form and a certificate upon execution of the Order Form and, after receipt of valid evidence of exemption, ServiceNow shall not charge Customer any Taxes from which it is exempt. If ServiceNow is required to invoice or collect Taxes associated with Customer's purchase of, payment for, access to or use of the Subscription Service or Professional Services, ServiceNow will issue an invoice to Customer including the amount of those Taxes, itemized where required by law. Customer shall provide to ServiceNow its VAT or GST identification number(s) on the Order Form for (i) the country where Customer has established its business and/or (ii) any other country where Customer has a fixed establishment. Customer shall use the ordered Subscription Service and Professional Services for Customer's business use in the foregoing location(s) in accordance with the provided VAT or GST identification number(s). The parties' obligations under this Section shall survive the termination or expiration of the Agreement.

2.3 USE VERIFICATION. Customer may not use or otherwise access the Subscription Service in a manner that exceeds Customer's authorized use. ServiceNow may review Customer's use of the Subscription Service, and Customer shall provide any reasonable assistance to verify Customer's compliance with the Agreement. If ServiceNow determines that Customer has exceeded its permitted use of the Subscription Service then ServiceNow will notify Customer and within thirty (30) days thereafter Customer shall either: (i) disable any unpermitted use or (ii) purchase additional subscriptions. If Customer fails to regain compliance within such thirty (30) day period, ServiceNow may suspend Customer's use of the Subscription Service or terminate the Agreement for cause in accordance with Section 7 (Term and Termination), in addition to any other rights or remedies ServiceNow may have.

3. GRANT OF USE RIGHTS; OWNERSHIP; CUSTOMER RESTRICTIONS

3.1. SUBSCRIPTION SERVICE. Customer is authorized to use the Subscription Service limited by the purchased amount and subscription term ("***Subscription Term***") on the Order Form and the Product Overview.

3.2. DOCUMENTATION. ServiceNow grants to Customer a non-exclusive, non-transferable, worldwide right during the Subscription Term to access and use the documentation relating to the operation and use of the Subscription Service that is provided by ServiceNow to Customer under the Agreement, as updated by ServiceNow from time to time ("***Documentation***").

3.3. CUSTOMER DATA. Customer grants ServiceNow a non-exclusive, non-transferable, worldwide right to use the electronic data pertaining to Customer and/or its users that is processed using the Subscription Service (collectively "***Customer Data***") strictly for the limited purpose of providing the Subscription Service to Customer.

3.4. SOFTWARE. ServiceNow may provide ServiceNow software products ("***Software***") for use in connection with the Subscription Service. Any Software is licensed and not sold (even if for convenience ServiceNow makes reference to words such as "sale" or "purchase"). ServiceNow grants Customer a limited, personal, worldwide, non-sublicensable, non-transferable, non-exclusive license to install and execute the Software on machines operated by or for Customer solely to permit Customer to use the Subscription Service during the Subscription Term in accordance with the terms and conditions of the Agreement. The Software may include code that is licensed under third party license agreements, including open source made available or provided with the Software.

3.5. OWNERSHIP. As between ServiceNow and Customer, all rights, title, and interest in and to all intellectual property rights in the Subscription Service, Software and/or Documentation are owned exclusively by ServiceNow. Except as expressly provided in the Agreement, ServiceNow does not grant Customer (and expressly reserves) any rights, express or implied, or ownership in the Subscription Service, Software and/or Documentation. ServiceNow shall have a royalty-free, worldwide, non-exclusive, transferable, sub-licensable, irrevocable, perpetual right to make, use, sell, offer for sale, import, or otherwise incorporate into the Subscription Service, Software and/or Documentation, any suggestions, enhancements, recommendations or other feedback provided by Customer relating to the Subscription Service, Software and/or Documentation.

3.6. RESTRICTIONS. Customer shall not (and shall not permit others to) do the following with respect to the Subscription Service, Software or Documentation: (i) license, sub-license, sell, re-sell, rent, lease, transfer, distribute or time share or otherwise make any of them available for access by third parties; (ii) disassemble, reverse engineer, decompile or modify them or otherwise create derivative works thereof; (iii) access them for the purpose of developing products or services that compete with the Subscription Service; (iv) use them to operate more or different type of applications or platform not authorized under the Agreement; (v) use them to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or engage in any other malicious act; (vi) disrupt their security, integrity or operation; (vii) remove or modify a copyright or other proprietary rights notice in them; (viii) use them to reproduce, distribute, display, transmit or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (ix) use them to damage the property of another; (x) use them in any manner which violates any law or regulation of the United States, any state thereof or other government authority; (xi) use them in any manner that disables, hacks or otherwise interferes with any security, digital signing, digital rights management, verification or authentication mechanisms or (xii) use them in a manner that temporarily or permanently alters, erases, removes, copies, modifies, halts or disables any ServiceNow or third party data, software or network.

4. WARRANTIES

4.1. LIMITED SUBSCRIPTION SERVICE WARRANTY. ServiceNow warrants that during the Subscription Term Customer's production instances of the Subscription Service shall materially conform to the Product Overview. To submit a warranty claim under this Section, Customer shall (1) reference this Section; and (2) submit a support request to resolve the non-conformity as provided in the Subscription Service Guide, which is set forth on www.servicenow.com/be_schedules.do. If the non-conformity persists without relief more than thirty (30) days after written notice of a warranty claim provided to

ServiceNow under this Section 4.1, then Customer may terminate the affected Subscription Service and ServiceNow shall refund to Customer any prepaid subscription fees covering the remainder of the Subscription Term of the affected Subscription Service after the date of termination. Notwithstanding the foregoing, this warranty shall not apply to any non-conformity due to a modification of or defect in the Subscription Service that is made or caused by any person other than ServiceNow or a person acting at ServiceNow's direction. THIS SECTION 4.1 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

4.2. LIMITED PROFESSIONAL SERVICES WARRANTY. ServiceNow warrants that the Professional Services will be performed in a competent and workmanlike manner in accordance with accepted industry standards and practices and all material requirements set forth in the SOW or Service Description. Customer shall notify ServiceNow in writing of any breach within thirty (30) days after performance of the non-conforming Professional Services. Upon receipt of such notice, ServiceNow, at its option, shall either use commercially reasonable efforts to re-perform the Professional Services in conformance with these warranty requirements or shall terminate the affected Professional Services and refund to Customer any amounts paid for the nonconforming Professional Services. THIS SECTION 4.2 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

4.3. DISCLAIMER OF WARRANTIES. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED IN THE AGREEMENT, TO THE MAXIMUM EXTENT ALLOWED BY LAW, SERVICENOW DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING WARRANTIES ARISING UNDER STATUTE, WARRANTIES OF MERCHANTABILITY, ACCURACY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTIES ARISING FROM USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SERVICENOW SPECIFICALLY DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE, SOFTWARE, PROFESSIONAL SERVICES OR DOCUMENTATION WILL MEET THE REQUIREMENTS OF CUSTOMER OR OTHERS OR THAT THEY WILL BE ACCURATE OR OPERATE WITHOUT INTERRUPTION OR ERROR. CUSTOMER ACKNOWLEDGES THAT IN ENTERING THE AGREEMENT IT HAS NOT RELIED ON ANY PROMISE, WARRANTY OR REPRESENTATION NOT EXPRESSLY SET FORTH HEREIN.

5. CONFIDENTIALITY AND NON-USE RESTRICTIONS

5.1. CONFIDENTIAL INFORMATION. "***Confidential Information***" means all information disclosed by a party ("***Disclosing Party***") to the other party ("***Receiving Party***"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of the disclosure, including without limitation: each party's respective business plans and processes; financial and employee data; proprietary technology and product information and designs; the Subscription Service and Software and Customer Data. The terms of the Agreement and Order form(s) are Confidential Information of ServiceNow. Confidential Information excludes information that: (i) is or becomes generally known to the public; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation to the Disclosing Party; (iii) is received from a third party without any obligation of confidentiality to a third party or breach of any obligation of confidentiality to the Disclosing Party; or (iv) was independently developed by the Receiving Party without reference to the Disclosing Party's Confidential Information.

5.2. PROTECTION. The Receiving Party shall: (i) at all times protect the confidentiality of the Disclosing Party's Confidential Information with the same degree of care that it uses to protect its own confidential information, and in no event using less than reasonable care; and (ii) not use Confidential Information of the Disclosing Party except to the extent necessary to exercise its rights or fulfill its obligations under the Agreement. To the extent necessary under the Agreement, the Receiving Party may disclose the Confidential Information of the Disclosing Party to the Receiving Party's employees or contractors who are bound by written obligations of confidentiality and non-use and non-disclosure restrictions at least as protective as those set forth herein. In the event of a court order or government regulation compelling disclosure of any Confidential Information, the Receiving Party shall provide the Disclosing Party with prompt written notice thereof, and shall reasonably cooperate with the Disclosing Party to seek confidential or other protective treatment. Each party's obligations set forth in this Section 5 shall remain in effect during the term and three (3) years after termination of the Agreement. The Receiving Party shall promptly return to the Disclosing Party or destroy (with certification of such destruction provided by the Receiving Party upon request) all Confidential Information of the Disclosing Party in its possession or control upon request from the Disclosing Party. Provisions for the return of Customer Data are set forth in Section 7.3 (Return of Customer Data).

6. LIMITATIONS OF LIABILITY AND DAMAGES

6.1. LIMITATIONS OF LIABILITY. TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY ARISING OUT OF OR RELATED TO The AGREEMENT OR THE SERVICES PROVIDED HEREUNDER, WHETHER BASED ON CONTRACT, IN TORT OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER FOR THE SERVICE GIVING RISE TO THE CLAIM DURING THE

TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS LIMIT. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO: (1) BODILY INJURY OR DEATH; (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; AND (3) CUSTOMER'S OBLIGATION TO PAY AMOUNTS OWED FOR SERVICES PROVIDED HEREUNDER.

6.2. EXCLUSION OF DAMAGES. TO THE EXTENT PERMITTED BY LAW, NEITHER SERVICENOW NOR CUSTOMER SHALL BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR LOST PROFITS (WHETHER DIRECT OR INDIRECT) OR LOSS OF USE OR DATA, COVER, SUBSTITUTE GOODS OR SERVICES, OR FOR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGE TO BUSINESS, REPUTATION OR GOODWILL), OR INDIRECT DAMAGES OF ANY TYPE HOWEVER CAUSED, WHETHER BY BREACH OF WARRANTY, BREACH OF CONTRACT, IN TORT OR ANY OTHER LEGAL OR EQUITABLE CAUSE OF ACTION EVEN IF SUCH PARTY HAS BEEN ADVISED OF SUCH DAMAGES IN ADVANCE OR IF SUCH DAMAGES WERE FORESEEABLE. THE FOREGOING EXCLUSIONS SHALL NOT APPLY TO: (1) BODILY INJURY OR DEATH; AND (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

7. TERM AND TERMINATION

7.1. TERM AND TERMINATION. The Agreement continues until terminated in accordance with its terms. Each party may terminate the Agreement in its entirety either: (i) upon thirty (30) days' prior written notice to the other party, if at the time such notice is served there are no Order Forms in effect; or (ii) upon written notice if the other party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership or liquidation, in any jurisdiction, that is not dismissed within sixty (60) days of its commencement or an assignment for the benefit of creditors. Either party may terminate a Subscription Service or Professional Services effective immediately upon written notice if the other party materially breaches a material obligation under the Agreement or the applicable Order Form for the affected service and does not cure the breach within thirty (30) days after receiving written notice thereof from the non-breaching party. Professional Services are separately ordered from the Subscription Service, and are not required for the Subscription Service. A breach by a party of its obligations with respect to Professional Services shall not by itself constitute a breach by that party of its obligations with respect to the Subscription Service even if the services are enumerated in the same Order Form.

7.2. EFFECT OF TERMINATION OF SERVICE. Upon expiration or other termination of the Subscription Service for any reason, Customer shall stop using, and ServiceNow shall stop providing, the terminated Subscription Service. (a) If the Subscription Service is terminated by Customer due to ServiceNow's breach, then ServiceNow shall refund to Customer, within thirty (30) days after the effective date of termination, all prepaid fees for the remaining portion of the Subscription Term for the terminated Subscription Service after the effective date of termination. (b) If Professional Service is terminated by Customer due to ServiceNow's breach, then ServiceNow shall refund to Customer, within thirty (30) days after the effective date of termination, any prepaid amounts for unperformed Professional Service. (c) If the Subscription Service is terminated by ServiceNow due to Customer's breach, then Customer shall pay to ServiceNow, within thirty (30) days after the effective date of termination, fees for the terminated Subscription Service that would have been payable for the remainder of the Subscription Term after the effective date of termination. (d) Upon expiration or other termination of the Subscription Service for any reason, Customer shall be eligible to request the return of Customer Data in accordance with Section 7.3 (Return of Customer Data).

7.3. RETURN OF CUSTOMER DATA. Following the end of the Subscription Term, where Customer has not renewed, Customer shall have forty-five (45) days to request a copy of the Customer Data from ServiceNow; and, if requested, ServiceNow shall use commercially reasonable efforts to provide a copy of that data within fifteen (15) days in a mutually agreed upon, commercially standard format at no cost to Customer unless ServiceNow determines in its reasonable discretion that the data output is not routine, in which case the parties shall mutually agree on a statement of work for professional services. After such forty-five (45) day period, ServiceNow shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of the Subscription Service.

7.4. SURVIVAL. Upon termination of the Agreement for any reason, Customer shall pay all amounts owed hereunder. Sections 3.5 (Ownership), 3.6 (Restrictions), and 5 (Confidentiality and Non-Use Restrictions) through 8 (General Provisions) of these General Terms and Conditions, together with any other provision required for their construction or enforcement, shall survive termination of the Agreement for any reason.

8. GENERAL PROVISIONS

8.1. ASSIGNMENT. Neither party may assign its rights or obligations, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the foregoing, either party may, upon notice and without the other party's consent: (i) in connection with a merger, reorganization or sale of all or substantially all of the assets or equity

of such party, assign the Agreement in its entirety to such party's successor; and (ii) assign the Agreement in its entirety to any company, partnership or other legal entity which from time to time directly or indirectly controls, is controlled by or is under the common control with such party. Any attempted or purported assignment in violation of this Section 8.1 will be null and void. Subject to the foregoing, the Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

8.2. NOTICE. Except as otherwise provided herein, all notices shall be in writing and deemed given upon: (i) personal delivery; (ii) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (iii) the second business day after mailing; or (iv) the first business day after sending by email, except that email shall not be sufficient for notices regarding a Claim. Notices shall be sent to the parties as set forth on the Order Form or as otherwise agreed to by the parties in writing.

8.3. EXPORT COMPLIANCE. Each party shall comply with United States and foreign export control laws and regulations. Customer acknowledges that the Subscription Service, Professional Services, Software and Documentation are subject to the U.S. Export Administration Regulations (the "***EAR***") and that Customer shall comply with the EAR. Without limiting the foregoing, Customer represents and warrants that: (i) Customer is not located in, and shall not use the Subscription Service, Professional Services, Software and Documentation from, any country that is subject to U.S. export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan and Syria); (ii) Customer shall not use the Subscription Service, Professional Services, Software and Documentation in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, sounding rockets or unmanned air vehicle systems; and (iii) Customer is not prohibited from participating in the U.S. export transactions by any federal agency of the U.S. government. In addition, Customer is responsible for complying with any local laws which may impact Customer's right to import, export or use the Subscription Service, Professional Services, Software and Documentation.

8.4. FORCE MAJEURE. No party shall be liable or responsible to the other party, nor be deemed to have defaulted under or breached the Agreement, for any failure or delay in fulfilling or performing any term of the Agreement, when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control, including without limitation: strikes, lock-outs or other industrial disputes (whether involving its own workforce or a third party's), trespassing, sabotage, theft or other criminal acts, failure of energy sources or transport network, acts of God, war, terrorism, riot, civil commotion, interference by civil or military authorities, national or international calamity, armed conflict, malicious damage, breakdown of plant or machinery, nuclear, chemical or biological contamination, explosions, collapse of building structures, fires, floods, storms, earthquakes, epidemics or similar events, natural disasters or extreme adverse weather conditions (each a "***Force Majeure Event***"). The party suffering a Force Majeure Event shall use reasonable efforts to mitigate against the effects of such Force Majeure Event.

8.5. US GOVERNMENT RIGHTS. All ServiceNow software is commercial computer software and all services are commercial items. "***Commercial computer software***" has the meaning set forth in Federal Acquisition Regulation ("***FAR***") 2.101 for civilian agency purchases and the Department of Defense ("***DOD***") FAR Supplement ("***DFARS***") 252.227-7014(a)(1) for defense agency purchases. If the software is licensed or the services are acquired by or on behalf of a civilian agency, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the services are acquired by or on behalf of any agency within the DOD, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses Government rights in computer software or technical data.

8.6. ENTIRETY. Customer acknowledges that it has not relied on any statement, promise or representation made or given by or on behalf of ServiceNow which is not set out in the Agreement. Customer's order is not contingent on, and Customer has not relied on, the delivery of any future functionality regardless of any verbal or written communication about ServiceNow's future plans. The Agreement supersedes all prior or contemporaneous oral or written agreement, representations and negotiations, including, but not limited to, any terms contained in Customer's purchase order.

8.7. WAIVER AND AMENDMENT. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of the Agreement, an Order Form, the Product Overview, the Subscription Service Guide, a SOW or a Service Description must be in writing and signed by authorized representatives of both parties.

8.8. RELATIONSHIP OF THE PARTIES. The parties are independent contractors. Nothing in the Agreement shall be construed to create a partnership, joint venture or agency relationship. Neither party shall have any right or authority

to assume or create any obligation of any kind expressed or implied in the name of or on behalf of the other party. ServiceNow may at any time subcontract or delegate in any manner any or all of its obligations under the Agreement to any third party or agent.

8.9. GOVERNING LAW; VENUE; TIME FOR BRINGING ACTION. The Agreement shall be governed by, subject to, and interpreted in accordance with the laws of the state of California, United States of America, if Customer is located in Canada, United States or Mexico, and the laws of England if Customer is located elsewhere. If Customer is located in Canada, United State or Mexico, the parties hereby irrevocably consent to the nonexclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in San Diego, California, or New York, New York, for the purposes of adjudicating any action or proceeding to enforce the terms of the Agreement. If Customer is located elsewhere, then any dispute arising under the Agreement shall be finally settled by binding arbitration in London, England. Such arbitration shall be conducted in English in accordance with the rules of the International Chamber of Commerce by one (1) arbitrator appointed in accordance with such rules. The arbitrator shall allow such discovery as is appropriate in accomplishing a fair, speedy, and cost-effective resolution of the dispute, and shall be expressly empowered to issue appropriate injunctive relief. The award of arbitration shall be final and binding upon both parties, and judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof. Any monetary award shall be payable in United States dollars. To the extent permitted by law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. No cause of action arising hereunder or relating hereto may be brought more than one (1) year after it first accrues. The prevailing party in an action to enforce the Agreement shall be entitled to costs of bringing the claim and reasonable attorneys' and experts' fees and expenses. Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's intellectual property rights.

8.10. CONSTRUCTION. The Subscription Service and Professional Services shall be provided in the English language unless agreed otherwise. The parties confirm that they have requested that the Agreement and all related documents be drafted in English at the express wishes of the parties. Les parties ont exigé que le présent contrat et ServiceNow les documents connexes soient rédigés en anglais selon la volonté expresse des parties. Capitalized terms not defined herein shall have the meaning set forth or referenced in the Subscription Service Guide. Section headings are for convenience only and are not to be used in interpreting the Agreement.

SUBSCRIPTION SERVICE GUIDE

Capitalized terms not defined herein shall have the meaning set forth in the Express General Terms and Conditions or Subscription Service Agreement.

1. CUSTOMER OPERATION OF SUBSCRIPTION SERVICE

1.1. PASSWORDS AND USER NAMES. Customer shall: (a) protect the names and passwords of users of the Subscription Service and prevent and notify ServiceNow of unauthorized use of the Subscription Service; (b) appoint up to five (5) designated support contacts for purposes of contacting ServiceNow support regarding questions and/or technical issues ("***Authorized Customer Support Contacts")*** and ensure that the Authorized Customer Support Contacts' information is current in the ServiceNow support portal; (c) be responsible for the lawfulness of, and results obtained from, all Customer Data submitted by users to the Subscription Service and each user's acts and omissions; and (d) use the Subscription Service only in accordance with the Documentation.

1.2. ACCESS CONTROL. ServiceNow provides the technical architecture that permits Customer to use and process Customer Data in the Subscription Service. This architecture includes an access control list engine. Customer shall be responsible for using the access control list engine for protecting all Personal Data. Customer shall ensure that access to and use of Subscription Service is restricted to only users authorized by Customer. Customer shall be responsible for ensuring all such users maintain the security of any passwords, usernames and other forms of authentication to the Subscription Service. A username and password must be uniquely assigned to a specific person and may not be shared by multiple persons at any one time or transferred. "***Personal Data***" means information identifying a natural person; an identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, financial, cultural or social identity.

2. SECURITY PROGRAM; EXCEPTIONS

ServiceNow shall maintain a security program ("***Security Program***") that includes industry standard practices designed to protect Customer Data from unauthorized access, use, disclosure, alteration, distribution and destruction. Notwithstanding anything to the contrary in this Agreement, the Security Program apply only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. The Security Program does not apply to: (i) information shared with ServiceNow that is not Customer Data; (ii) Customer Data in transit over the Internet, Customer's virtual private network (VPN), or another third party network; (iii) any Customer Data processed by Customer or its users in violation of this Agreement; or (iv) any part of the Subscription Service that is not hosted by ServiceNow.

3. UPGRADES

3.1. UPGRADES. "***Upgrades***" are ServiceNow's releases of the Subscription Service for repairs, enhancements or new features applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term. ServiceNow has the discretion to provide new functionality either: (i) as an Upgrade, or (ii) as different software or service for a separate fee. ServiceNow determines whether and when to develop, release and apply any Upgrade to Customer's instances of the Subscription Service.

3.2. MAINTENANCE. ServiceNow shall use reasonable efforts to give Customer ten (10) days' notice of any service maintenance to the infrastructure network, hardware or software used by ServiceNow to operate and deliver the Subscription Service if ServiceNow, in its reasonable judgment, believes that such cloud infrastructure maintenance will impact Customer's use of its production instances of the Subscription Service. ServiceNow will use reasonable efforts to limit the Maintenance Time (as defined below) to no more than two (2) hours per month. Notwithstanding the foregoing, ServiceNow may provide Customer with a shorter or no notice period of service maintenance if necessary, in the reasonable judgment of ServiceNow, to maintain the availability, security, stability or performance of the Subscription Service.

4. SUPPORT

During the Subscription Term, ServiceNow shall use reasonable efforts to resolve Defects in the Subscription Service ("***Support***").

A "***Defect***" means a problem causing the Subscription Service to not conform to the Product Overview. Customer may request Support for a Defect at the online portal https://hi.service-now.com/ or any successor site.

A Defect will be assigned a priority level as follows:

- A Priority Level 1 Defect is any Defect that causes Customer's instance(s) of the Subscription Service to be not Available (as defined below).
- A Priority Level 2 Defect is any Defect that causes a mission critical function of the Subscription Service to fail.
- A Priority Level 3 Defect is any Defect that significantly impedes work or progress.
- A Priority Level 4 Defect is any Defect that does not significantly impede work or progress.

Upon notification by Customer of a Defect, ServiceNow shall, in all instances, target an initial response (the "***Initial Response***") within the timeframes set forth in the Support Table, as measured from the time that Customer notifies ServiceNow. The initial response from ServiceNow shall include, as applicable and without limitation: (i) ServiceNow's acknowledgment or notification to Customer of such Defect, and (ii) the classification of such Defect as a Priority Level 1, 2, 3 or 4.

SUPPORT TABLE

Priority Level	Target Initial Response
1	30 minutes; at all times
2	2 hours; at all times
3	Within 1 business day
4	Varies

Support does not include: implementation services; configuration services; integration services; customization services or other custom software development; support for modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction; training or "how-to"; assistance with administrative functions; professional services; corrections of immaterial Defects or Defects that have a viable workaround; or corrections that will degrade the Subscription Service.

5. SERVICE LEVEL OBJECTIVE

5.1. DEFINITIONS.

(a) "***Available***" means that the Subscription Service can be accessed by authorized users.

(b) "***Excused Downtime***": means (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays not within ServiceNow's control, and network intrusions or denial-of-service or other criminal attacks.

(c) "***Maintenance Time***" means the time the Subscription Service is not Available due to service maintenance.

(d) "***Availability Service Level Objective***" means the percentage of total time during which Customer's production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime.

5.2. AVAILABLITY. ServiceNow shall use reasonable efforts to provide an Availability Service Level Objective of 99.8% over any calendar month. There is no service credit offered for a failure to meet this Availability Service Level Objective.

SCHEDULE A

TERMS AND CONDITIONS TO
VIRTRU PRO
SUBSCRIPTION AGREEMENT

1. DEFINITIONS

For purposes of this Agreement, the following terms shall have the following meanings:

1.1 "**Derivative Work**" shall mean a new or modified work that is based on or derived from a preexisting work, including, without limitation, a work that, in the absence of a license, would infringe the copyright in such preexisting work or that uses trade secrets or other proprietary information with respect to such preexisting work.

1.2 "**Materials**" shall mean the Virtru Pro software (including any object code, executable files, or browser plug-ins) or materials related thereto provided by Virtru to Customer hereunder, including, without limitation, any software downloaded from Virtru's website or from the Virtru Pro Services; any related materials and documentation therefor; and any modifications, error corrections, bug fixes, new releases, enhanced functionality (including platform integration features not generally available to non-commercial users of Virtru's software) or other updates thereto that may be provided hereunder by Virtru to Customer during the term of this Agreement.

1.3 "**Third Party Services**" shall mean any services used in connection with the Materials that are hosted by a party other than Virtru or Licensee.

1.4 "**Virtru Pro Services**" shall mean the Virtru hosted services made available by Virtru to Customer in connection with the Materials.

2. RIGHTS IN MATERIALS AND TO USE SERVICE

2.1 Grant of Rights. Subject to the terms and conditions of this Agreement, Virtru (a) hereby grants to Customer a restricted, non-exclusive, nontransferable, nonsublicensable, royalty-free (except as set forth in Section 2.3), revocable right to use, during the term of this Agreement and in accordance with the documentation provided by Virtru, the Materials (the **"License"**), and (b) Virtru will make the Virtru Pro Services available to Customer pursuant to this Agreement during the term of this Agreement. Except as set forth in this Section 2.1, no other right or license of any kind is granted by Virtru to Customer hereunder with respect to the Materials or the Virtru Pro Services. Customer acknowledges and agrees that, unless otherwise agreed in writing between the parties, Customer shall be solely responsible for procuring and complying with any license or right to use any Third Party Services, including those offered by Customer's email services provider.

2.2 Restrictions. Customer shall not, without the prior written consent of Virtru: (a) copy all or any portion of the Materials or Virtru Pro Services; (b) decompile, disassemble, scrape or otherwise reverse engineer the Materials, Virtru Pro Services or any portion thereof, or determine or attempt to determine any source code, algorithms, methods or techniques embodied in the Materials or used in the Virtru Pro Services or any portion thereof; (c) modify, translate or create any Derivative Works based upon the Materials or Virtru Pro Services; (d) distribute, disclose, market, rent, lease, assign, sublicense, pledge or otherwise transfer the Materials, in whole or in part, to any third party or export the Materials outside the United States; (e) remove or alter any copyright, trademark, trade name or other proprietary notices, legends, symbols or labels appearing on or in copies of the Materials or the Virtru Pro Services; (f) perform, or release the results of, benchmark tests or other comparisons of the Materials or Virtru Pro Services with other programs or services; (g) transfer the Materials to any computer other than a computer owned by Customer and used by Customer in Customer's operations; (h) permit the Materials or Virtru Pro Services to be used for processing the data of any third party; (i) incorporate the Materials, Virtru Pro Services or any portion thereof into any other program, product or service, or use the Materials or Virtru Pro Services to provide similar services or functionality to third parties; (j) provide any third party with access to the Virtru Pro Services other than as expressly permitted herein or by the Terms of Service (as defined below); (k) use the Materials or Virtru Pro Services for any unlawful or tortious purpose; or (l) use the Materials or Virtru Pro Services for any purpose other than in accordance with the terms and conditions of this Agreement or Virtru's then-current terms of service (available at https://www.virtru.com/terms-of-service) (the "**Terms of Service**"). Customer shall ensure that all Customer end users of the Virtru Pro Service and Materials comply with

the terms and conditions of this Agreement. Customer shall be responsible for compliance with this Agreement by each Customer end user and it shall monitor and manage all Customer users in connection with this Agreement.

2.3 Fees; Payment. In consideration of the Virtru's provision of the Virtru Pro Services and Materials, Customer shall make payments to Virtru in accordance with the terms set forth on the cover page of this Agreement. Sales and use tax, VAT, or GST are Customer's sole responsibility, and Customer acknowledges and agrees that all fees are exclusive of all such taxes.

2.4 Seats; Reporting. Customer shall initially be permitted to use the Materials and Virtru Pro Services with respect to the number of seats set forth on the cover page of this Agreement (the "**Baseline Seat Count**"). Each seat shall be used by one Customer user. During the term of this Agreement, Customer will report to Virtru the total number of users of the Materials and Virtru Pro Services on an annual basis. Such report will be submitted to sales@virtru.com and shall be due thirty (30) days prior to each anniversary of the date of this Agreement (each, a "**Reporting Date**") based on the actual number of users as of the date thirty (30) days prior to such Reporting Date (each, a "**Seat Count Date**"). If the actual number of Customer users as of any Seat Count Date is higher than the Baseline Seat Count, Customer will pay the "Subscription Fee per Seat" set forth on the cover page of this Agreement (the "**Subscription Fee**") for each such additional user for any Renewal Term.

2.5 Adjustment Events. In addition to the annual reporting required under Section 2.4 above, Customer shall report to Virtru any increase of ten percent (10%) or more in the aggregate number of Customer users in excess of the Baseline Seat Count that occurs between Reporting Dates (an "**Adjustment Event**") and agrees to pay Virtru, within thirty (30) days following any such Adjustment Event, a prorated Subscription Fee for each such additional user for the remaining portion of the applicable term and for any Renewal Term.

2.6 Seat Count Audit. At any time during the term of this Agreement, Virtru shall have the right to audit Customer's usage of the Virtru Pro Services and Materials (a "**Seat Count Audit**"). If the actual number of Customer users as of the date of any Seat Count Audit is higher than the Baseline Seat Count, Customer will pay the "Subscription Fee per Seat" set forth on the cover page of this Agreement for the remaining portion of the applicable term and for any Renewal Term.

3. SUPPORT

Virtru will provide support to Customer and its end users through Virtru's generally available online ticketing and support system. Except as expressly provided in Schedule B, which is incorporated herein by reference, in this Section 3 or as may otherwise be provided under a written support agreement entered into by Virtru and Customer, Virtru is under no obligation to support the Materials or Virtru Pro Services in any way, nor to provide any modification, error correction, bug fix, new release or other update (each an "**Update**") to or for the Materials or Virtru Pro Service. In the event Virtru, in its sole discretion, supplies or makes available any Update to Customer, such Update shall be deemed to be part of the Materials or Virtru Pro Services (as applicable) hereunder and shall be subject to the terms and conditions of this Agreement.

4. PROPRIETARY RIGHTS

4.1 General. As between Virtru and Customer, Virtru retains all right, title and interest, including, without limitation, all patent rights, copyrights, trademarks and trade secrets, in and to the Materials, Virtru Pro Services and any portion thereof, including, without limitation, any copy or Derivative Work of the Materials, Virtru Pro Services or any portion thereof and any Update thereto. Customer agrees to take any action reasonably requested by Virtru to evidence, maintain, enforce or defend the foregoing. Customer shall not take any action to jeopardize, limit or interfere in any manner with Virtru's ownership of and rights with respect to the Materials, Virtru Pro Services or any Derivative Work or Update. Customer shall have only those rights in or to the Materials, Virtru Pro Services and any Derivative Work or Update granted to it pursuant to this Agreement.

4.2 Feedback. Customer and its authorized users may provide suggestions, requests, recommendations and other feedback concerning Customer's use of the Materials and Virtru Pro Services (including, without limitation, any errors or difficulties discovered with respect thereto) (the "**Feedback**"). Customer agrees that all Feedback shall be the sole

property of Virtru and Virtru may use such Feedback at its discretion without the consent of Customer.

5. PROPRIETARY INFORMATION

5.1 Proprietary Information. Both parties acknowledge that, in the course of this Agreement each may obtain confidential or proprietary information of the other party ("**Proprietary Information**"). "Proprietary Information" will include, without limitation, (a) the existence of and terms of this Agreement, (b) trade secrets, know-how, inventions (whether or not patentable), techniques, processes, programs (whether in source code or object code form), ideas, algorithms, formulas, schematics, testing procedures, software design and architecture, computer code, documentation, design and functional specifications, product requirements, problem reports, performance information, software documents, hardware, devices, designs, drawings, unpublished patent applications, data, plans, strategies and forecasts, and (c) technical, engineering, manufacturing, product, marketing, servicing, financial, personnel and other information. Virtru's "Proprietary Information" will include, without limitation, the Materials (including all Derivative Works and Updates) and all confidential information related thereto provided by Virtru to Customer in connection with this Agreement. Virtru's Proprietary Information shall, as between Customer and Virtru, belong solely to Virtru, and Customer's Proprietary Information shall, as between Customer and Virtru, belong solely to Customer.

5.2 Use and Disclosure Restrictions. Each party agrees (a) to protect the other party's Proprietary Information from unauthorized dissemination and use; (b) to use the other party's Proprietary Information only for the performance of this Agreement and the exercise of any rights under this Agreement; (c) not to disclose any Proprietary Information, or any part or parts thereof, to any of its employees, agents, contractors or any other individuals except to its employees who are under confidentiality obligations no less restrictive than the requirements of this Section 5; (d) with respect to Customer, not to disclose or otherwise provide to any third party, without the prior written consent of Virtru or as otherwise set forth in a separate written agreement between the parties hereto entered into after the date hereof, as applicable, any of Virtru's Proprietary Information, materials or any data or other information produced, obtained or created by Customer in connection with Customer's use of the Materials, including, without limitation, the existence of this Agreement and the existence and possible applications of the Materials; (e) to undertake whatever action is necessary (or authorize the other party to do so in the name of such party) to prevent or remedy any breach of such party's confidentiality obligations herein set forth or any other unauthorized disclosure of any Proprietary Information by its current or former employees, agents or contractors; and (f) not to remove or destroy any proprietary or confidential legends or markings placed upon or contained within the Proprietary Information provided to such party by the other party.

5.3 Exclusions. The foregoing restrictions on disclosure and use shall not apply with respect to any Proprietary Information that: (a) is or becomes publicly known through no act or omission of the other party; (b) was rightfully known by the receiving party without confidential or proprietary restriction before receipt from the other party, as evidenced by the receiving party's contemporaneous written records; (c) becomes rightfully known to the receiving party without confidential or proprietary restriction from a source other than the disclosing party that does not owe a duty of confidentiality with respect to such Proprietary Information; or (d) is independently developed without the use of the Proprietary Information as evidenced by the receiving party's written records. In addition, a party may use or disclose Proprietary Information to the extent (i) approved in writing by the other party and (ii) a party is legally compelled to disclose such Proprietary Information, provided, however, that prior to any such compelled disclosure, such party shall cooperate fully with the other party in protecting against any such disclosure and/or obtaining a protective order narrowing the scope of such disclosure and/or use of the Proprietary Information. Further, each party may disclose the terms and conditions of this Agreement: (A) in confidence, to legal counsel; (B) in confidence, to accountants, banks, and financing sources and their advisors; and (C) in connection with the enforcement of this Agreement or any rights hereunder.

5.4 Equitable Relief. Each party agrees that, due to the unique nature of the other party's Proprietary Information, the unauthorized disclosure or use of the other party's Proprietary Information or any other breach of any provision of this Section 5 will cause irreparable harm and significant injury to the other party, the extent of which will be difficult to ascertain and for which there will be no adequate remedy at law. Accordingly, each party agrees that the other party, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of this Section 6 without the necessity of posting any bond or other security. Each party shall notify the other party in writing immediately upon becoming aware of any such breach or threatened breach.

6. NO WARRANTY

THE MATERIALS AND VIRTRU PRO SERVICES ARE PROVIDED "AS IS" AND VIRTRU DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS OR IMPLIED, RELATING TO THE MATERIALS AND VIRTRU PRO SERVICES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT OF THIRD PARTY RIGHTS, OR WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE OR TRADE PRACTICE. VIRTRU DOES NOT GUARANTEE THE ACCURACY OF THE INFORMATION INCLUDED IN, TRANSMITTED THROUGH OR MADE AVAILABLE BY THE MATERIALS OR VIRTRU PRO SERVICES, WHICH MAY INCLUDE INACCURACIES OR ERRORS. VIRTRU DOES NOT GUARANTEE THAT THE MATERIALS OR VIRTRU PRO SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT BUGS OR MALFUNCTIONS WILL BE CORRECTED OR THAT THE MATERIALS, VIRTRU PRO SERVICES OR VIRTRU'S SERVERS ARE FREE OF HARMFUL COMPONENTS. VIRTRU DOES NOT GUARANTEE THAT THE MATERIALS OR VIRTRU PRO SERVICES ARE ACCURATE, WITHOUT ERROR OR RELIABLE.

7. VIRTRU'S ENTIRE LIABILITY

TO THE EXTENT ALLOWED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (a) IN NO EVENT SHALL VIRTRU OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INADVERTENT DISCLOSURE OF DATA, OR INTERRUPTION OF BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND OR OTHER ECONOMIC LOSS ARISING FROM OR RELATING TO THIS AGREEMENT OR THE SUBJECT HEREOF, EVEN IF VIRTRU HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, HOWEVER CAUSED, AND (b) NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, VIRTRU'S ENTIRE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT OR THE SUBJECT HEREOF, UNDER ANY LEGAL THEORY (WHETHER IN CONTRACT, TORT, INDEMNITY OR OTHERWISE), IF ANY, SHALL NOT EXCEED ONE THOUSAND DOLLARS (US$1,000).

8. INDEMNIFICATION

Customer shall defend, indemnify and hold Virtru harmless against any loss, liability, damage or cost (including reasonable attorneys' fees) in connection with claims, actions, demands, suits, or proceedings made or brought against Virtru by a third party alleging (a) that any modification or addition to the Materials or Virtru Pro Services made by or for Customer (other than by Virtru) infringes a copyright, mask work right, trade secret, trademark right or patent of the third party; (b) in combination with any other product or service not provided, specified or recommended in writing by Virtru for use with the Materials or Virtru Pro Services; or (b) with respect to the development, manufacture, marketing, sales, distribution or use of any of the Materials or Virtru Pro Services, including, without limitation, a product liability claim or a claim for breach of any warranty or support obligations. In connection with a claim under this Section 9, Virtru shall: (i) provide Customer with prompt notice of the claim; (ii) permit Customer to control the defense and any settlement of the claim (provided that Customer may not settle any claim unless such settlement unconditionally releases Virtru of all liability in connection with such claim); and (iii) provide cooperation as reasonably requested by Customer (at Customer's expense).

9. TERM AND TERMINATION

9.1 Term. This Agreement shall commence on the Effective Date and, unless sooner terminated pursuant to the terms hereof, shall continue in full force and effect for one (1) year (the "**Initial Term**"). Thereafter, this Agreement shall automatically renew for successive one (1) year periods (each a "**Renewal Term**"), unless either party provides the other party with written notice of its intent not to renew at least thirty (30) days prior to the end of the then-current term. The automatic renewal of this Agreement will be for the Baseline Seat Count, as adjusted pursuant to Sections 2.4, 2.5 and/or 2.6, on the same payment terms as set forth on the cover page of this Agreement.

9.2 Termination. Either party may terminate this Agreement immediately upon written notice to the other party if the other party fails to perform any of its duties or obligations hereunder and, except with respect to Customer's breach of Section 2.1 or 2.2, which breach shall not be subject to any cure period, fails to cure such default within thirty (30) days following receipt of written notice from the non-defaulting party specifying the occurrence or existence of the default. Customer shall notify Virtru within twenty-four (24) hours of Customer becoming aware of any breach (other than by Virtru) of the terms and conditions of this Agreement, including, without limitation, Sections 2 and 5.

9.3 Effect of Termination. Upon the expiration or termination of this Agreement, the rights granted to Customer hereunder shall terminate, Customer will cease all use of the Materials, return to Virtru or destroy the Materials in its possession, and, upon Virtru's request, so certify such actions to Virtru. Any costs

incurred in returning or destroying the Materials upon termination shall be borne by Customer. The provisions of Sections 2.2, 4.2, 5, 6, 7, 8, 9.3, and 10 shall survive the expiration or any termination of this Agreement. Termination of this Agreement by either party shall not act as a waiver of any breach of this Agreement and shall not act as a release of either party from any liability for breach of such party's obligations under this Agreement. Neither party shall be liable to the other for damages of any kind solely as a result of terminating this Agreement in accordance with its terms, and termination of this Agreement by a party shall be without prejudice to any other right or remedy of such party under this Agreement or applicable law.

10. GENERAL PROVISIONS

10.1 Notices. Any notice, request, demand or other communication required or permitted hereunder shall be in writing, shall reference this Agreement and shall be deemed to be properly given: (a) when delivered personally; (b) seven (7) days after having been sent by registered or certified mail, return receipt requested, postage prepaid; or (c) two (2) business days after deposit with a private industry express courier, with written confirmation of receipt. All notices shall be sent to the address set forth on the cover page of this Agreement and to the notice of the person executing this Agreement (or to such other address as may be designated by a party by giving written notice to the other party pursuant to this Section 10.1).

10.2 Assignment. This Agreement may not be assigned, in whole or part, whether voluntarily, by operation of law or otherwise, by Customer without the prior written consent of Virtru. Subject to the preceding sentence, the rights and liabilities of the parties hereto shall bind, and inure to the benefit of, their respective assignees and successors and is binding on the parties and their successors and assigns. Any attempted assignment other than in accordance with this Section 10.2 shall be null and void.

10.3 Governing Law, Jurisdiction and Venue. This Agreement is to be construed in accordance with and governed by the internal laws of the Commonwealth of Virginia (but expressly excluding the Uniform Computer Information Transactions Act ("**UCITA**") as enacted in Virginia) without giving effect to any choice of law rule that would cause the application of the laws of any jurisdiction other than the internal laws of the Commonwealth of Virginia (excluding UCITA) to the rights and duties of the parties. Any legal suit, action or proceeding arising out of or relating to this Agreement shall be commenced in a federal court in the Eastern District of Virginia or in state courts with jurisdiction over Fairfax County**,** Virginia, and each party hereto irrevocably submits to the exclusive jurisdiction and venue of any such court in any such suit, action or proceeding.

10.4 Attorneys' Fees. If any legal action, including, without limitation, an action for arbitration or injunctive relief, is brought relating to this Agreement or the breach hereof, the prevailing party in any final judgment or arbitration award, or the non-dismissing party in the event of a dismissal without prejudice, shall be entitled to the full amount of all reasonable expenses, including all court costs, arbitration fees and actual attorneys' fees paid or incurred in good faith.

10.5 Waiver. The waiver by either party of a breach of or a default under any provision of this Agreement, shall be in writing and shall not be construed as a waiver of any subsequent breach of or default under the same or any other provision of this Agreement, nor shall any delay or omission on the part of either party to exercise or avail itself of any right or remedy that it has or may have hereunder operate as a waiver of any right or remedy.

10.6 Severability. If the application of any provision of this Agreement to any particular facts or circumstances shall be held to be invalid or unenforceable by an arbitration panel or a court of competent jurisdiction, then (a) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of this Agreement shall not in any way be affected or impaired thereby and (b) such provision shall be enforced to the maximum extent possible so as to effect the intent of the parties and reformed without further action by the parties to the extent necessary to make such provision valid and enforceable.

10.7 Relationship of the Parties. Nothing contained in this Agreement shall be deemed or construed as creating a joint venture, partnership, agency, employment or fiduciary relationship between the parties. Neither party nor its agents have any authority of any kind to bind the other party in any respect whatsoever, and the relationship of the parties is, and at all times shall continue to be, that of independent contractors.

10.8 Restricted Rights. If Customer is an agency or instrumentality of the United States Government, the Materials are "commercial computer software" and "commercial computer software documentation," and, pursuant to FAR 12.212 or DFARS 227.7202, and their successors, as applicable, use reproduction and disclosure of the Materials are governed by the terms of this Agreement.

10.9 Reference. Customer agrees to serve as a "reference customer" that may be disclosed by Virtru to third parties (including by displaying Customer's name, logo and/or a link to Customer's web site on Virtru's web site) and, upon reasonable notice from Virtru, shall serve as a reference to potential customers, vendors, investors, or other third parties designated by Virtru; provided, however, that Virtru shall provide Customer with reasonable prior notice of its need to have Customer serve as a reference.

10.10 Entire Agreement. This Agreement, any Schedules and any Exhibits attached hereto and incorporated herein by reference, and the Terms of Service constitute the entire agreement between the parties concerning the subject matter hereof and supersede all prior or contemporaneous representations, discussions, proposals, negotiations, conditions, agreements and communications, whether oral or written, between the parties relating to the subject matter of this Agreement and all past courses of dealing or industry custom. No amendment or modification of any provision of this Agreement shall be effective unless in writing and signed by a duly authorized signatory of each of Virtru and Customer.

10.11 Counterparts and Electronic Signatures. The Parties may execute this Agreement in counterparts, each of which is deemed an original, but all of which together constitute one and the same agreement. This Agreement may be delivered electronically or by facsimile transmission, and the parties hereby agree that any electronic or facsimile signatures hereto are legal, valid and enforceable as originals.

SCHEDULE B

MAINTENANCE AND SUPPORT SERVICES SCHEDULE

1. DEFINITIONS

For purposes of this Schedule, the following term shall have the following meaning:

(a) "**Support Services**" means the delivery of front-end support to Customer's end users by telephone, email or other methods and the training of Customer's end users, in each case relating to the use of the Materials and Virtru Pro Services.

2. SUPPORT SERVICES.

Virtru will be responsible for providing Customer's end users with Support Services. Virtru will not be required to provide the Support Services if Customer has failed to pay any amount payable to Virtru under this Agreement and such amount is more than thirty (30) days overdue.

3. UPDATES.

Virtru will provide Customer with one copy of each Update made generally available by Virtru to its customers that pay for customer support and maintenance during the term of this Agreement.

4. SUPPORT HOURS.

Virtru will provide the Support Services during Virtru's normal business hours, Monday to Friday, except holidays. Virtru will respond to Customer support inquiries or requests within one business day.

vCloud Air (U.S. and Japan Data Centers)

TERMS OF SERVICE

Last updated: November 5, 2014

VMware vCloud Air is an infrastructure as a service offering. By accessing any service offered through VMware vCloud Air (the " **Service Offering**") you agree to be bound by these terms of service between you and VMware (" **Agreement**"). If you do not agree to this Agreement, you must not access the Service Offering. An individual accepting this Agreement on behalf of an organization represents and warrants having legal authority to bind that organization. " **You**" means the entity accepting this Agreement. " **VMware**," " **we**," or " **us**" means VMware, Inc., a Delaware corporation, to the extent that you are purchasing the Service Offering in the United States, VMware vCloud Service G.K., a company organized and existing under the laws of Japan, to the extent that you are purchasing the Service Offering in Japan, and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you are purchasing the Service Offering elsewhere. Capitalized terms used in this Agreement are defined throughout this Agreement and in Section 14.

EVALUATION PROGRAM USE. When you access the Service Offering under a VMware evaluation program, you may use the Service Offering only for non-production computing activity. Notwithstanding any other provision in this Agreement, under a VMware evaluation program, we provide the Service Offering "AS-IS" without indemnification, support or warranty of any kind, expressed or implied, and we will not be liable for any damages. Upon termination of the evaluation, you will no longer have access to the Service Offering and Your Content.

1. The Service Offering.

1.1 Generally. This Agreement governs your access and use of the Service Offering. We may deliver the Service Offering to you with the assistance of our affiliates, licensors and providers. Service Level Agreements may apply to the Service Offering. You will comply with all laws, rules and regulations applicable to your use of the Service Offering, and with the Third Party Terms, the Service Description, the Privacy Addendum, and the Support Policy, all of which are incorporated herein by reference.

1.2 Access to the Service Offering. You may access and use the Service Offering solely for your own benefit and only in accordance with this Agreement. To access the Service Offering, you must register for the Service Offering and set up an authorized account with Login Credentials. You may monitor and manage your Service Offering account via the My VMware Portal available at www.vmware.com/accounts and through the Service Offering Portal available at http://vcloud.vmware.com. You must keep confidential your Login Credentials. If you set up an authorized account for an organization, you will require that all authorized users of that account (including anyone providing services to you) keep confidential their Login Credentials. You will keep your registration information accurate, complete and current as long as you use the Service Offering. You are responsible for any use that occurs under your Login Credentials, including any activities by you, or your employees, contractors or agents. If you believe an unauthorized user has gained access to your Login Credentials, you will notify us as soon as possible. Neither we nor our affiliates are responsible for any unauthorized access to or use of your account.

1.3 Verifying; Cooperation. We have the right to verify your compliance with this Agreement. If we

seek to verify that compliance, you will provide information or other materials reasonably requested by us to assist the verification. We monitor the overall performance and stability of the infrastructure of the Service Offering. You may not block or interfere with that monitoring. If we reasonably believe a problem with the Service Offering may be attributable to Your Content or your use of the Service Offering, you will cooperate with us to identify and resolve the source of that problem.

1.4 Additional Terms; Third Party Content. As part of your use of the Service Offering, you may receive access to additional data, content, software or applications subject to separate terms. If so, those separate terms will prevail over this Agreement as to your use of that data, content, software or applications. Third Party Content is available "AS IS" without indemnification or support, and we disclaim all express and implied warranties (including warranties of merchantability, fitness for a particular purpose, and non-infringement). You are responsible for reviewing, accepting, and complying with any third party terms of use or other restrictions applicable to the Third Party Content. Those terms will be available to you through a notification within the Service Offering or in a document available at https://www.vmware.com/files/pdf/support/vmware-vcloud-air-third-party-terms.pdf. It is your responsibility to check the Third Party Terms, which may be modified from time to time. We may provide billing and related services associated with the Third Party Content. We will not provide any support for the Third Party Content unless otherwise noted in the Third Party Terms. We reserve the right to suspend or terminate the Third Party Content at any time, but we will use commercially reasonable efforts to provide reasonable notice of that suspension or termination.

1.5 Early Evaluation/Beta Features. We may identify and make available on an early evaluation or beta basis certain features or functionality within the Service Offering. You must use these features or functionality only for evaluation purposes and for the period that we specify. We provide these features and functions "AS-IS," without indemnification or support and disclaim all express and implied warranties (including warranties of merchantability, fitness for a particular purpose, and non-infringement). Any early evaluation or beta features or functionality do not constitute an implied commitment to offer to you or anyone these features and functionality as part of the Service Offering on a generally available basis.

1.6 Open Source Software. You may receive open source software when you use the Service Offering and any open source software distributed to you is made available under the applicable open source license, which can be found at: http://www.vmware.com/download/open_source.html. You may obtain a copy of these licenses and any source code (and modifications) that we are required to make available under these licenses (the " **Source Files**") at http://www.vmware.com/download/open_source.html or by sending a written request, with your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All written requests must clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you last received open source software as part of the Service Offering or last accessed the Service Offering.

2. Data Protection and Security.

2.1 Data Protection. We will process personal data contained in Your Content as set forth in the Privacy Addendum.

2.2 Your Content and Security. You are solely responsible for Your Content. You are responsible for protecting the security of Your Content, including any access you might provide to Your Content by your employees, customers or other third parties, and in transit to and from the Service Offering. The Service Offering provides you with certain software and functionality to help you protect Your Content from unauthorized access. You will take and maintain appropriate security, protection and backup of Your Content, which might include the use of encryption technology to protect Your Content from unauthorized access. You are responsible for providing any necessary notices to your

users and obtaining any legally-required consents from your users concerning their use of the Service Offering. You are solely responsible for complying with any laws or regulations that might apply to Your Content. You are responsible for any losses or other consequences arising from your failure to encrypt or back up Your Content.

3. Acceptable Use.

3.1 General Restrictions. You and those accessing the Service Offering through you may not: (a) resell or sublicense the Service Offering; or (b) use or access the Service Offering: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate any rights of others; (iii) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Service Offering or any other service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the Service Offering or impair anyone else's use of it; (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees or usage limits; or (vii) in any application or situation where failure of the Service Offering could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage. You must ensure that your users comply with the terms of this Agreement, and you agree that if you become aware of any violation by one of your users, you will terminate that user's access to Your Content immediately. If we have reason to believe that you or your users have breached this Agreement, we or our designated representative may review your use of the Service Offering, including your account, Your Content, and your records, to verify your compliance with this Agreement.

3.2 Content Restrictions. You will take steps to ensure that those accessing any service you provide with the Service Offering do not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; or (e) contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships. You are solely responsible for any software, product or service that a third party licenses, sells or makes available to you that you install or use with the Service Offering. Your use of that software, product or service is governed by separate terms between you and that third party. We are not a party to and are not bound by any of those separate terms. You represent and warrant that Your Content does not and will not violate any third-party rights, including any Intellectual Property Rights, and rights of publicity and privacy. You will ensure that your use of the Service Offering complies at all times with your privacy policies and all applicable laws and regulations, including any encryption requirements.

3.3 Violations of Acceptable Use. If you become aware that any of Your Content or your user's use of Your Content violates Section 3.1 or 3.2, you will take immediate action to remove the applicable part of Your Content or suspend the end user's access. If you fail to do so, we may ask you to do so. If you fail to comply with our request within twenty-four hours, we may suspend your account or disable access to Your Content until you comply with our request.

3.4 Notification of Infringement Concerns. If you believe that your copyrighted work has been copied and is accessible on our Service Offering in a way that constitutes copyright infringement, please send a notice to us as further detailed in Section 8 of the Community Terms of Use available at http://www.vmware.com/community_terms.html.

4. IP Ownership.

4.1 Ownership of Service Offering. We and our licensors own and retain all right, title and interest in and to the Service Offering and any related VMware Software, including all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein. This includes any information that we collect and analyze in connection with the Service Offering, such as usage patterns, user feedback and other information to improve and evolve our software products and services offerings. Your rights to use the Service Offering are limited to those expressly granted in this Agreement. No other rights with respect to the Service Offering, any related VMware Software, or any related Intellectual Property Rights are implied.

4.2 Ownership of Your Content. You and your authorized users retain all right, title and interest in and to Your Content and all Intellectual Property Rights therein. Our rights to access and use Your Content are limited to those expressly granted in this Agreement. No other rights with respect to Your Content or any related Intellectual Property Rights are implied.

4.3. Feedback. We will be free to use for any purpose any feedback (such as comments or suggestions) that you provide to us regarding the Service Offering. You hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, perform, display, disclose, distribute, modify, prepare derivative works of and otherwise exploit the feedback without restriction in any manner now known or in the future conceived and to make, use, sell, offer to sell, import and export any product or service that incorporates the feedback.

5. Order, Delivery, Payment, and Taxes.

5.1 Generally. Sections 5.3 (Direct Orders), 5.4 (Delivery), 5.5 (Invoicing and Payment Terms) and 5.6 (Taxes) apply only to orders you place directly with, and the Service Offering you purchase directly from, VMware. When ordering through, or purchasing the Service Offering from, a VMware authorized reseller, the authorized reseller might specify similar terms.

5.2 Orders. All Orders issued to VMware are subject to the terms of this Agreement and are not binding until accepted by VMware. We are not required to provide any Service Offering to you until you provide all information we require for processing your Order.

5.3 Direct Orders. For orders placed directly with VMware, you must issue a purchase order to VMware for the initial Service Offering order, but a purchase order is not required for the monthly billings that occur after the initial Order billing. For subsequent billings, all fees (including subscription renewals, metered usage components, and other add-ons) will be paid in accordance with this Agreement. Your Order will be deemed accepted when we authorize the purchased Service Offering for your Login Credentials.

5.4 Delivery. When VMware accepts your Order for the Service Offering, we will deliver the corresponding Login Credentials to you by email to the address associated with your account. If VMware ships a physical object in connection with an add-on feature of the Service Offering, shipping and delivery terms are Ex Works VMware's regional fulfillment facility (INCOTERMS 2010).

5.5 Invoicing and Payment Terms. You will pay all fees for use of the Service Offering in the amount and currency specified in your invoice, within 30 days after the date of the invoice, and regardless of your usage level during a billing period. You will also be responsible for all additional fees for any subscription renewals and metered usage components consumed, and other subscriptions, features, products, services or add-ons that you purchase within the Service Offering. You will be billed in advance for the monthly or prepaid charges due to the subscription services purchased. Any metered usage components and any initial monthly fees will be billed in arrears. The applicable fees for subscriptions (including renewals), features and other available products and

services will be governed by the then-current applicable price list at the time the initial, renewal, or add-on order is submitted, or as otherwise agreed. We may increase or add new fees for the Service Offering by notifying you at least 30 days in advance.

5.6 Taxes. Service Offering fees are exclusive of taxes, and you shall pay or reimburse for all taxes arising out of transactions contemplated by this Agreement. If you are required to pay or withhold any tax for payments due under this Agreement, you shall gross your payments to us so we receive sums due in full and free of any deductions. You will provide documentation to us showing that taxes have been paid to the relevant taxing authority. " **Taxes**" means any sales, VAT, use, gross receipts, business and occupation, and other taxes (other than taxes on our income), export and import fees, customs duties and similar charges imposed by any government or other authority. You hereby confirm that we can rely on the name and address you provide to us when you agree to the Service Offering or in connection with your payment method as being the place of supply for sales tax and income tax purposes or as being the place of supply for VAT purposes where you have established your business.

6. Temporary Suspension.

6.1 Generally. Upon prior written notice to you, we may suspend your use of the Service Offering if we reasonably determine: (a) payment for the Service Offering is not received within 30 days from the date on which payment is due; (b) you or your use of the Service Offering is in breach of this Agreement; (c) you fail to address our request to take action as specified in Section 3.3; (d) your use of the Service Offering poses a security risk to the Service Offering or other users of the Service Offering; or (e) suspension is required pursuant to our receipt of a subpoena, court order, or other request by a law enforcement agency.

6.2 Effect of Suspension. You will remain responsible for all fees incurred before or during the suspension. You will not be entitled to any service credits under the Service Level Agreement that you might have otherwise accrued during the period of suspension.

7. Term and Termination.

7.1 Term of Agreement. This Agreement will be in effect through the Subscription Term, plus any renewals, unless terminated earlier as permitted under this Agreement or the Service Description. Upon the completion of the Subscription Term, the subscription will automatically renew as specified in the Service Description, unless terminated as permitted under the Service Description.

7.2 Termination for Cause. We may terminate this Agreement effective immediately upon sending you an email notice if: (a) you breach any provision in Sections 3.1 or 3.2; (b) you do not resolve the underlying cause resulting in a suspension of your account pursuant to Section 6.1 (other than suspension due to a subpoena, court order, or other request by a law enforcement agency) within 10 days after your account is suspended; or (c) you commit a material breach that cannot be cured.

7.3 Termination for Insolvency. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) terminate or suspend your business; (b) become insolvent, admit in writing your inability to pay your debts as they mature, make an assignment for the benefit of creditors; or (c) become subject to control of a trustee, receiver or similar authority or any bankruptcy or insolvency proceeding.

7.4 Effect of Termination. Upon the termination of this Agreement for any reason: (a) all rights granted to you under this Agreement, including your ability to access the Service Offering, will immediately terminate; and (b) you must promptly discontinue all use of the Service Offering and delete or destroy any of our Confidential Information. We will retain Your Content for a period of 30

days following the effective date of the termination, although you will cease to have access to the Service Offering or Your Content during this period. After the 30 days, Your Content will be deleted. Sections 1.6 (Open Source Software), 3 (Acceptable Use) 4 (IP Ownership), 5 (Order, Delivery, Payment and Taxes), 7 (Term and Termination), 9 (Disclaimer), 11 (Limitation of Liability), 12 (Confidential Information), 13 (General), and 14 (Definitions), will survive the termination of this Agreement. Termination of the Service Offering (except to the extent that the termination is permitted under Section 13.3 of this Agreement or Section 3.6 of the Service Description) will not entitle you to any refunds, credits, or exchanges, and you will be liable for all monthly billing fees for the remainder of the Subscription Term after termination, as well as all usage and other fees incurred up to the termination date.

8. Support and Subscription Services. When applicable, and subject to the terms of this Agreement, we will provide to you support for the Service Offering in accordance with the terms specified in the Support Policy. We will not provide support to any end users of Your Content.

9. Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE AND OUR LICENSORS AND SERVICE PROVIDERS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE REGARDING OR RELATING TO THE SERVICE OFFERING OR ANY MATERIALS OR SERVICES FURNISHED OR PROVIDED TO YOU UNDER THIS AGREEMENT. WE AND OUR LICENSORS AND SERVICE PROVIDERS DO NOT WARRANT THAT THE SERVICE OFFERING WILL BE UNINTERRUPTED OR FREE FROM DEFECTS, OR THAT THE SERVICE OFFERING WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

10. Indemnification.

10.1 Indemnification by Customer. You will defend and indemnify us against any third party claim arising from or relating to: (a) Your Content; (b) any infringement or misappropriation of any Intellectual Property Rights by you, your customers, your end users or your suppliers; (c) violation of law by you; (d) your use of the Service Offering (including any activities under your account and any use by your employees, personnel or end users) in violation of this Agreement, or (e) your use of any Third Party Content. We will (a) provide you with notice of the claim within a reasonable period of time after learning of the claim; and (b) reasonably cooperate in response to your requests for assistance. You may not settle or compromise any indemnified claim without our prior written consent.

10.2 Defense and Indemnification. Subject to the remainder of this Section 10, we will defend you against an Infringement Claim and indemnify you from the resulting costs and damages finally awarded against you to that third party by a court of competent jurisdiction or agreed to in settlement. You will (a) provide us with notice of any Infringement Claim within a reasonable period of time after learning of it; (b) allow us sole control over the claim's defense and settlement; and (c) reasonably cooperate in response to our requests for assistance. You may not settle or compromise any Infringement Claim without our prior written consent.

10.3 Remedies. If the Service Offering becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will at our option and expense either: (a) procure the rights necessary for you to keep using the Service Offering; (b) modify or replace the Service Offering to make it non-infringing; or (c) terminate this Agreement and refund any pre-paid fees for the Service Offering pro-rated for its remaining Subscription Term.

10.4 Exclusions. We will have no obligation under this Section 10 or otherwise with respect to any

claim based on: (a) a combination of VMware Software with non-VMware products or content, including Your Content; (b) use of the Service Offering for a purpose or in a manner not specified in this Agreement or the Service Description; (c) any modification to the Service Offering made without our express written approval; or (d) any Service Offering provided on a no charge basis. This Section 10 states your exclusive remedy for any infringement actions or claims.

11. Limitation of Liability.

11.1 Generally. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE OR OUR LICENSORS OR SERVICE PROVIDERS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. IN ADDITION, OUR AND OUR LICENSORS' AND SERVICE PROVIDERS' LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF: (A) THE AGGREGATE FEES PAID OR PAYABLE TO US FOR YOUR ACCESS TO AND USE OF THE SERVICE OFFERING IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO YOUR CLAIM, OR (B) $5,000 USD (OR THE EQUIVALENT IN LOCAL CURRENCY). REGARDLESS OF WHETHER WE OR OUR LICENSORS OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THESE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO (A) VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT OR (B) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY APPLICABLE LAW.

11.2 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

12. Confidential Information.

12.1 Protection. A party may use Confidential Information of the other party solely to exercise its rights and perform its obligations under this Agreement or as otherwise permitted under this Agreement. Each party will disclose the Confidential Information of the other party only to the employees, service providers or contractors of the recipient party who have a need to know the Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than each party's duty hereunder. Each party will use reasonable care to protect the confidentiality of the other party's Confidential Information.

12.2 Exceptions. The recipient's obligations under Section 12.1 with respect to any Confidential Information will terminate if the recipient can show by written records that the information: (a) was already known to the recipient at the time of disclosure by the other party; (b) was disclosed to the recipient by a third party who had the right to make the disclosure without any confidentiality restrictions; (c) is, or through no fault of the recipient has become, generally available to the public; or (d) was independently developed by the recipient without access to, or use of, discloser's Confidential Information. The recipient may disclose Confidential Information to the extent the disclosure is required by law or regulation. The recipient will provide the other party notice, when practicable, and will take reasonable steps to contest and limit the scope of any required disclosure.

13. General.

13.1 Assignment. You may not assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without our prior written consent. Any attempted assignment or transfer without that consent will be void. Subject to these limits, this Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.

13.2 Notices. Any notice delivered by us to you under this Agreement will be delivered by email to the email address associated with your account or by posting on either the Service Offering Portal or the My VMware Portal, except as otherwise set forth in this Agreement. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

13.3 Modifications. We may change periodically the Service Offering, the terms of your access to the Service Offering, this Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy. It is your responsibility to regularly check the Service Offering console and the My VMware portal for updates. We will notify you of any material, detrimental change to this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. The modified Agreement, Service Description, Privacy Addendum, Service Level Agreement, or Support Policy, as applicable, will become effective as of the date stated in that notification. If we make a material, detrimental change to the Service Offering (other than the termination or modification of any beta feature or functionality), this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy, then you may terminate this Agreement within 30 days of the change to the Service Offering or within 30 days of the notification. In that event, the termination will be effective as of the date we receive your notification, unless you state an effective date in your notification that is within 45 days after we receive your notification. In the event of that termination, we will refund any prepaid fees, pro-rated for the remainder of your Subscription Term, and less any discounts that would then not be earned. Your continued use of the Service Offering after the effective date of any modification to the Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy will be deemed acceptance of the modified terms, as applicable.

13.4 Waiver. The waiver of a breach of any provision of this Agreement will not constitute a waiver of any other provision or any later breach.

13.5 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in force.

13.6 Compliance with Laws; Export Control. Each party will comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Service Offering is of United States origin, is provided subject to the U.S. Export Administration Regulations (including "deemed export" and "deemed re-export" regulations), and may be subject to the export control laws of the applicable territory. You represent and warrant that (a) you are not, and are not acting on behalf of, (1) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; (b) you will not permit the Service Offering to be used for any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons; (c) Your Content will not be classified or listed on the United States Munitions list, contain defense articles, defense services or contain ITAR-related data; (d) Your Content will not require an export license and is not restricted from export to any VMware global resource or personnel under applicable export control laws; and (e) you are not subject, either directly or indirectly, to any order

issued by any agency of the United States government, revoking or denying, in whole or in part, your United States export privileges. You will notify VMware immediately if you become subject to any such order.

13.7 Government Regulations. For purposes of sales to government entities in the U.S.: The Service Offering and its documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFARS Section 227.7202 and FAR Paragraph 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Service Offering and documentation by or on behalf of the U.S. Government will be governed solely by the terms and conditions of this Agreement.

13.8 Force Majeure. We will not be liable for any delay or failure to perform any obligations under this Agreement due to any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war.

13.9 Construction. The headings of sections of this Agreement are for convenience and are not for use in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

13.10 Governing Law. This Agreement is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), except as follows: To the extent that you choose a Japan data center Service Offering, then this Agreement is governed by the laws of Japan (excluding its conflict of law rules). The United Nations Convention for the International Sale of Goods does not apply.

13.11 Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.12 Order of Precedence. The terms of this Agreement will supersede and control over any conflicting or additional terms and conditions of any other purchasing related document issued by you.

13.13 Entire Agreement. This Agreement, as may be revised by us, is the entire agreement of the parties regarding its subject matter. This Agreement supersedes all prior or contemporaneous communications, understandings and agreements, whether written or oral, between the parties regarding its subject matter.

14. Definitions.

14.1 "Confidential Information" means non-public technical, business or other information or materials disclosed or otherwise made available by one party that are in tangible form and labeled "confidential" or the like, or, information which is provided under circumstances reasonably indicating their confidentiality. Our Confidential Information includes: (1) Login Credentials; and (2) any information or materials relating to the Service Offering.

14.2 "Infringement Claim" means any third party claim that any VMware Software used to provide the Service Offering infringes any patent, trademark or copyright of the third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area; (d) Australia; (e) New Zealand; (f) Japan; or (g) the People's Republic of China, to the extent that those

countries are part of your places of use of the Service Offering.

14.3 "Intellectual Property Rights" means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, patent applications, and moral rights, whether registered or unregistered.

14.4 "Login Credentials"mean any passwords, authentication keys or security credentials that enable your access to and management of the Service Offering.

14.5 "Order" means the internet order page, order document, purchase order, or purchase agreement issued to VMware that specifies your purchase of the Service Offering.

14.6 "Privacy Addendum" means the then-current version of the Service Offering Data Privacy Addendum document available at http://vcloud.vmware.com/legal, which we may modify from time to time.

14.7 "Service Description" means the then-current Service Offering Service Description document available at https://www.vmware.com/files/pdf/vcloud-air/vcloud-air-Service-Description.pdf, which contains technical and other information and which we may modify from time to time.

14.8 "Service Level Agreement" means the then-current Service Level Agreement document available at https://www.vmware.com/support/vcloud-air/sla.html, which we may modify from time to time.

14.9 "Subscription Term" means the time period of your access to the Service Offering, as specified by your Order.

14.10 "Support Policy" means the then-current version of the Service Offering Support Policy document available at http://www.vmware.com/support/services/iaas-production.html, which we may modify from time to time.

14.11 "Third Party Content" means third party data, service, content, software or applications, including open source software.

14.12 "Third Party Terms" means the then-current version of the third party license terms applicable to the Service Offering that are available at https://www.vmware.com/files/pdf/support/vmware-vcloud-air-third-party-terms.pdf, which we may modify from time to time.

14.14 "VMware Software" means the software programs listed in our commercial price list.

14.15 "Your Content" means any and all applications, files, information, data or other content uploaded to or published or displayed through the Service Offering by you, your users, us (acting upon your instructions as part of a service), or any third party users who access any service you provide with the Service Offering.

sidepath

Quotation

22892 Mill Creek Drive
Laguna Hills, CA 92653
Phone (949) 748-8700; Fax (949) 748-8706
www.sidepath.com

Date: 09/02/26

Quotation #: SIDQ61812-01
Valid Until: 10/15/26
Prepared By: Catherine Paull
Project ID: SIDPROJECT57853

Bill To:

City of Redlands
Attn: Accounts Payable
35 Cajon Street
Redlands, CA 92373

Phone: (909) 798-7516
Email: accountspayable@cityofredlands.org

Ship To:

City of Redlands
Attn: Allen Fincher
35 Cajon Street
Redlands, CA 92373

Phone: 909) 307-7302
Email: afincher@cityofredlands.org

Qty	Part Number	Description	Unit Price	Total
		NASPO Master Agreement AR2472 - Contract Number 7-17-70-40-05		
		Option1: 1 Year - The Current Support for the Palo Alto items listed below expire on 10/15/2026. The Support Renewal will cover from 10/16/2026 to 10/15/2027.		
		Serial# 026901003246		
1	PAN-PA-1420-PAA-HA2-R	PA-1420, Prisma Access Agent subscription, for one (1) device in an HA pair, 1 year (12 months) term, renewal. (Serial# 026901003246)	$3,169.89	$3,169.89
1	PAN-PA-1420-BND-PRECISIONAI-R	PA-1420, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term (Serial# 026901003246)	$18,175.43	$18,175.43
1	PAN-SVC-PREM-1420-R	PA-1420, Premium support, 1 year (12 months) term, renewal. (Serial# 026901003246)	$3,898.35	$3,898.35
		Serial# 026901003266		
1	PAN-PA-1420-PAA-HA2-R	PA-1420, Prisma Access Agent subscription, for one (1) device in an HA pair, 1 year (12 months) term, renewal. (Serial# 026901003266)	$3,182.25	$3,182.25
1	PAN-PA-1420-BND-PRECISIONAI-R	PA-1420, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term (Serial# 026901003266)	$18,175.43	$18,175.43
1	PAN-SVC-PREM-1420-R	PA-1420, Premium support, 1 year (12 months) term, renewal. (Serial# 026901003266)	$3,898.35	$3,898.35
		Serial# 026901003267		
1	PAN-PA-1420-PAA-HA2-R	PA-1420, Prisma Access Agent subscription, for one (1) device in an HA pair, 1 year (12 months) term, renewal. (Serial# 026901003267)	$3,182.25	$3,182.25
1	PAN-PA-1420-BND-PRECISIONAI-R	PA-1420, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term (Serial# 026901003267)	$18,175.43	$18,175.43
1	PAN-SVC-PREM-1420-R	PA-1420, Premium support, 1 year (12 months) term, renewal. (Serial# 026901003267)	$3,898.35	$3,898.35
		Serial# 026901003276		

Qty	Part Number	Description	Unit Price	Total
1	PAN-PA-1420-BND-PRECISIONAI-R	PA-1420, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term (Serial# 026901003276)	$18,175.43	$18,175.43
1	PAN-PA-1420-PAA-HA2-R	PA-1420, Prisma Access Agent subscription, for one (1) device in an HA pair, 1 year (12 months) term, renewal. (Serial# 026901003276)	$3,169.89	$3,169.89
1	PAN-SVC-PREM-1420-R	PA-1420, Premium support, 1 year (12 months) term, renewal. (Serial# 026901003276)	$3,898.35	$3,898.35
			SubTotal	**$100,999.40**

Grand Total	**$100,999.40**

Terms and Conditions are identical to those currently in force.
Payment Terms from Ship Date/Order Placement Date: Net 30

If you have any questions regarding this quotation, please contact:

Krunal Patel
(949) 396-3743
krunal@sidepath.com

THANK YOU FOR YOUR BUSINESS!

PORTFOLIO SNAPSHOT

PORTFOLIO TITLE: Cloud Solutions
LEAD STATE: Utah

OVERVIEW:

The Master Agreements with sixty-two (62) suppliers in this portfolio offer a diverse range of XaaS cloud solutions and associated services.

INITIAL TERM: 09/02/2016 to 09/15/2026*

RENEWALS: None

TOTAL POSSIBLE TERM: Ten (10) years

*Due to differences in the date of execution and other factors, individual master agreement terms may vary. Buyers should review the applicable master agreement and associated addenda to verify the term.

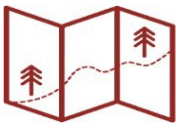
PRODUCT CATEGORIES:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

SUPPLIERS AVAILABLE (AS OF MARCH 2021):

Supplier	SaaS	PaaS	IaaS
8x8	X		
A&T Systems			X
Accenture	X	X	X
Armedia	X	X	
AT&T	X	X	X
ATOS	X	X	X
B2Gnow (dba of AskReply)	X		
Broadvoice	X		
Calibre	X		
Capgemini	X		
Carahsoft	X	X	X
CDW-G	X	X	X
CGI	X		X
CherryRoad Technologies		X	X
Cisco Systems	X	X	X
CodeLynx	X		
Collab9	X		
Companion Data Services	X		
Confi-Chek (formerly Enformion)	X		
Contact Solutions	X		
CSRA	X	X	X
Deloitte Consulting (assigned from Day 1 Solutions)	X	X	X
DLT Solutions	X	X	X

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.



DXC Technology Services	X	X	X
EC America (subsidiary of immixGroup)			X
ECS Federal (assigned from InfoReliance)	X		X
eGlobal Tech			X
EMC		X	X
Emergent	X	X	X
Enquizit	X		
Ensono			X
ESRI	X	X	X
eSolutionsGroup	X		
Experian	X		
Hewlett Packard Enterprise	X	X	X
HRTec	X	X	X
Hyland	X		
i2m (dba of Include Information Management)	X	X	X
IBM	X	X	X
Insight Public Sector	X	X	X
Knowledge Services (dba of GuideSoft)	X		
Laserfiche	X		
Lumen (dba of CenturyLink)	X	X	X
NTT Data			X
NWN	X		
Oracle	X	X	X
Presidio	X		
Quest	X		
Red River	X	X	X
Retarus	X		
SHI	X	X	X
Smartronix	X	X	X
Strategic Communications	X	X	X
TCC Software Solutions	X	X	X
Teradata		X	
Unisys	X	X	X
ViON	X	X	X
Visionary Integration Professionals	X		
VMware	X		X
WellSky (formerly Mediware Human & Social Services)	X		
Workday	X		
Zivaro (formerly Global Technology Resources)	X		

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.

PORTFOLIO SNAPSHOT

KEY BENEFITS:

- Master Agreements provide Participating Entities with access to technical capabilities that run in cloud environments and meet the NIST Essential Characteristics.
- Offerings are available from direct OEM providers, aggregators, business partners, and resellers to provide a full range of cloud-based solutions and services.
- Data security was a major component of the RFP, evaluation process, and Master Agreements.

PRICING:

Minimum percentage discounts for each product category are applied to each supplier's catalog, which can be found by clicking on the contractor tiles on the NASPO ValuePoint Cloud Solutions portfolio landing page. Customers may negotiate deeper discounts.

PROCUREMENT BACKGROUND:

Cloud Solutions was a new NASPO ValuePoint contract portfolio when established in 2016. The RFP allows the Lead State to conduct "refresh" solicitations bi-annually at its discretion to allow additional vendors to compete for a contract within the portfolio. The most recent refresh took place in 2018.

STATES ON SOURCING TEAM:

- ★ Utah (Lead)
- ★ Colorado
- ★ New Jersey
- ★ Tennessee
- ★ Vermont
- ★ Wisconsin

SOLICITATION INFORMATION (ORIGINAL):

- ✓ Type: Request for Proposal (RFP)
- ✓ Solicitation Number: CH16012
- ✓ Publicly Advertised: 12/21/2015 – 3/20/2016
- ✓ Posted On: Utah BidSync account (closed)
- ✓ Posting Link: No longer accessible
- ✓ Number of Days Publicly Posted: 90
- ✓ Number of Amendments Posted: 10

PUBLIC OPENING (ORIGINAL):

Sealed responses were unsealed upon closing of the solicitation at 1:00pm MT on 3/20/2016.

VENDOR RESPONSES (ORIGINAL):

- Number of Vendor Responses Received: 58
- Number of Non-Responsive Vendor Responses: 6
- Number of Vendor Responses Evaluated: 29

SOLICITATION INFORMATION (2018 REFRESH):

- ✓ Type: Request for Proposal (RFP)
- ✓ Solicitation Number: SK18008
- ✓ Publicly Advertised: 4/2/2018 – 7/6/2018
- ✓ Posted On: Utah Public Procurement Portal Place
- ✓ Posting Link: SK18008
- ✓ Number of Days Publicly Posted: 95
- ✓ Number of Amendments Posted: 6

PUBLIC OPENING (2018 REFRESH):

Sealed responses were unsealed upon closing of the solicitation at 3:00pm MT on 7/6/2018.

VENDOR RESPONSES (2018 REFRESH):

- Number of Vendor Responses Received: 80
- Number of Non-Responsive Vendor Responses: 5
- Number of Vendor Responses Evaluated: 75

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.

EVALUATIONS:

Responses to the original solicitation were evaluated by the members of the Sourcing Team during the week of 7/25/2016 in Salt Lake City, Utah. Responses to the 2018 refresh solicitation were evaluated by the members of the Sourcing Team during the week of 12/10/2018 in Salt Lake City, Utah.

EVALUATION CRITERIA:

Responses were evaluated based on the following Evaluation Criteria:

Business Information

1. Business Profile
2. Scope of Experience
3. General Information
4. Billing and Pricing Practices
5. Scope and Variety of Cloud Solutions
6. Best Practices

Organization & Staffing

1. Contract Manager

Organization & Staffing

1. Technical Requirements
2. Subcontractors
3. Working with Purchasing Entities
4. Customer Service
5. Security of Information
6. Privacy and Security
7. Migration and Redeployment Plan
8. Service or Data Recovery
9. Data Protection
10. Service Level Agreements
11. Data Disposal
12. Performance Measures and Reporting
13. Cloud Security Alliance
14. Service Provisioning
15. Back up and Disaster Plan
16. Solution Administration
17. Hosting and Provisioning
18. Trial and Testing Periods
19. Integration and Customization
20. Marketing Plan
21. Value-Added Services
22. Supporting Infrastructure
23. Alignment of Cloud Computing

SCORING:

Responses were scored according to the RFP's Evaluation Criteria across one technical evaluation stage, which included a minimum technical scoring threshold, and the cost evaluation. Detailed scoring information can be found in the Cloud Solutions Award Justification Statements posted on the NASPO ValuePoint Cloud Solutions portfolio landing page.

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.

PORTFOLIO SNAPSHOT

AWARD:

The original RFP allowed for multiple vendor awards in each award category based on each vendor's success in earning more than 70% of the maximum 1,325 total points possible (for IaaS and PaaS) and 1,275 total points possible (for SaaS). 38 of the 58 vendors evaluated met the required minimum score threshold in one or more categories, making them eligible for award.

The 2018 refresh RFP allowed for multiple vendor awards in each award category based on each vendor's success in earning more than 70% of the maximum 1,333.3 total points possible (for IaaS and PaaS) and 1,283.3 total points possible (for SaaS). 33 of the 80 vendors evaluated met the required minimum score threshold in one or more categories, making them eligible for award. This includes a number of vendors that were awarded a contract through the original RFP and were awarded additional categories through the refresh.

PUBLIC POSTING OF AWARD (ORIGINAL):

- Award Posted: 9/1/2016
- Posting Link: Award Justification Statement
- Vendors Awarded: 38
- Protests Received: 0

AWARDED VENDORS (ORIGINAL):

- A&T Systems
- AT&T
- ATOS
- Broadvoice
- Carahsoft
- CDW-G
- CGI
- CherryRoad Technologies
- Cisco Systems
- Collab9
- Contact Solutions
- CSRA
- Deloitte Consulting (assigned from Day 1 Solutions)
- DLT Solutions
- EC America (subsidiary of immixGroup)
- ECS Federal (assigned from InfoReliance)
- EMC
- Emergent
- ESRI
- FireEye
- IBM
- Insight Public Sector
- Knowledge Services (dba of GuideSoft)
- Logicworks
- Lumen (dba of CenturyLink)
- NTT Data
- Oracle
- Quest
- Retarus
- SHI
- Smartronix
- Strategic Communications
- TCC Software Solutions
- Teradata
- Unisys
- Verizon
- VMware
- Workday

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.

PUBLIC POSTING OF AWARD (2018 REFRESH):

- Award Posted: 1/23/2019
- Posting Link: Award Justification Statement
- Vendors Awarded: 33
- Protests Received: 8

AWARDED VENDORS (2018 REFRESH):

- 8x8
- Accenture
- Armedia
- AT&T
- B2Gnow (dba of AskReply)
- Calibre
- Capgemini
- CherryRoad Technologies
- CodeLynx
- Companion Data Services
- Confi-Chek (formerly Enformion)
- DXC Technology Services
- ECS Federal (assigned from InfoReliance)
- eGlobal Tech
- EMC
- Enquizit
- Ensono
- eSolutionsGroup
- Experian
- Hewlett Packard Enterprise
- HRTec
- Hyland
- i2m (dba of Include Information Management)
- IBM
- Laserfiche
- NWN
- PCMG (acquired by Insight Public Sector)
- Presidio
- Red River
- ViON
- Visionary Integration Professionals
- WellSky (formerly Mediware Human & Social Services)
- Zivaro (formerly Global Technology Resources)

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.

City Council **AGENDA ITEM NO. I5.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve an Assignment of Trademark and Domain Name with the Redlands Historical Museum Association and determine that approval is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines (Assistant City Manager Garcia)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council approve the Assignment of Trademark and Domain Name with the Redlands Historical Museum Association; authorize the Mayor to execute the agreement; and determine that approval of the agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines.

RECOMMENDATION:

Staff recommends that the City Council approve the Assignment of Trademark and Domain Name with the Redlands Historical Museum Association (RHMA), authorize the Mayor to execute the agreement, and determine that approval is exempt from environmental review pursuant to Section 15061(b)(3) of the State CEQA Guidelines.

DISCUSSION:

On June 17, 2025, the City and RHMA entered into a Real Estate Transfer Agreement through which RHMA transferred the Museum of Redlands property to the City. The agreement also provided for the transfer of branding rights associated with the Museum of Redlands trademark and RHMA's execution of a separate assignment to memorialize that transfer.

The proposed Assignment of Trademark and Domain Name confirms and completes the transfer to the City of all rights, title, and interest held by RHMA, if any, in the Museum of Redlands trademark, with or without its colors, together with the associated goodwill. RHMA would retain a non-exclusive right to use the mark on its letterhead, website, and other media, provided that the name "Redlands Historical Museum Association," "MOR Friends," or "Museum of Redlands Friends" appears prominently near the mark and its use complies with the City's reasonable quality-control requirements.

The agreement also assigns RHMA's rights and interests in the internet domain name themor.org to the City. RHMA would be required to take the actions reasonably necessary to complete the transfer to a City-controlled account, including providing required authorization information and approving applicable registrar requests. Following transfer, the City would be responsible for administration, maintenance, and renewal of the domain name.

ALTERNATIVES:

The Council may choose to modify, reject or table this item.

STRATEGIC PLAN:

The Museum of Redlands supports Strategic Priority A (Quality of Life) by preserving local history and providing educational, cultural, and community programming.

SUBMITTED BY:
Danielle Garcia, Assistant City Manager

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

FISCAL IMPACT

Fiscal Year: 2027

Discussion: The proposed assignment does not require payment to RHMA. Following transfer of the domain name, the Library would assume responsibility for applicable domain-registration and renewal costs.

Attachments

MOR_Trademark_Assignment_Agreement.pdf

ASSIGNMENT OF TRADEMARK AND DOMAIN NAME

This ASSIGNMENT OF TRADEMARK AND DOMAIN NAME ("Assignment") is made this 6th day of October, 2026, by and between Redlands Historical Museum Association ("Assignor"), a California nonprofit public benefit corporation, on the one hand, and the City of Redlands ("Assignee"), a California municipal corporation and general law city, on the other hand (each a "Party" and together the "Parties").

RECITALS

A. WHEREAS, Assignee desires to memorialize the assignment by Assignor to Assignee the below reproduced trademark comprising both word and design elements (the "Mark"):

In particular, the Mark comprises the capitalized letters "M," "O," and "R" forming the acronym "M.O.R.," which stands for Museum of Redlands, the letter "O" being represented by a circle, the acronym being disposed within a larger circle, the letters being positioned towards a lower right section of the circle such that the right leg of the letter "R" interrupts a perimeter of the circle. The letters are shaded in white, and the large circle is shaded in orange.

B. WHEREAS, pursuant to the Real Estate Transfer Agreement entered into by the Parties on June 17, 2025, and its exhibits, Assignor transferred to Assignee "all branding rights associated with the [Mark] and agree[d] to execute [this Assignment] to effectuate such transfer as may be reasonably requested by [Assignee]," which is the objective of this Assignment.

C. WHEREAS, Assignee has acquired all of Assignor's rights, title, and interest, if any, in and to the Mark, with and without its colors, including the goodwill associated therewith.

D. WHEREAS, Assignor has assigned to Assignee all of Assignor's rights, title, and interest, if any, in and to the Mark, with and without its colors, including the goodwill associated therewith.

E. WHEREAS, Assignor is the registered holder of, or otherwise possesses the authority to transfer, the Internet domain name themor.org ("the Domain Name"), and the Parties desire that all of Assignor's rights and interests in the Domain Name be transferred to Assignee.

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged as well as in the Real Estate Transfer Agreement of June 17, 2025, the Parties agree as follows:

TERMS AND CONDITIONS

1. Assignment of Mark. Assignor has assigned to Assignee all right, title, and interest Assignor had, if any, in and to the Mark, with and without its colors, together with the goodwill of the business symbolized by the Mark, all rights of action, powers, and benefits belonging or accrued to the Mark. To the extent any right, title, or interest in or to the Mark remains in Assignor, Assignor hereby irrevocably assigns and transfers the same to Assignee, together with the goodwill of the business symbolized by the Mark. Assignor shall execute and deliver such further documents, and take such further actions, as Assignee may reasonably request, at Assignee's expense, to confirm, perfect, or record Assignee's ownership of the Mark, including any document required by the United States Patent and Trademark Office or the California Secretary of State.

2. Assignment and Transfer of Domain Name. Assignor hereby assigns and transfers to Assignee all of Assignor's right, title, and interest in and to the Domain Name, including all rights arising from or associated with its registration. Assignor shall promptly take all actions reasonably necessary to complete the transfer of the Domain Name to an account designated and controlled by Assignee, including unlocking the Domain Name, providing any required authorization or transfer code, approving any change-of-registrant or registrar-transfer request, and executing any additional documents reasonably required by the applicable domain registrar.

Following completion of the transfer, Assignee shall be responsible for the administration, maintenance, and renewal of the Domain Name.

3. Assignor's Rights. Assignor shall have the non-exclusive right to use the Mark on its letterhead, website, and other media, provided the name "Redlands Historical Museum Association," "MOR Friends," or "Museum of Redlands Friends" appears prominently in close proximity to the Mark. Any use of the Mark by Assignor under this Section shall be subject to Assignee's reasonable quality-control requirements. The Parties agree that use of any such name satisfies the naming condition applicable to Assignor's continued use of the Mark under Section 2.1(C) of the Real Estate Transfer Agreement, which is modified accordingly, and that Assignor's use of "MOR Friends" or "Museum of Redlands Friends" as its name in accordance with this Section is permitted notwithstanding Assignee's rights in the name "Museum of Redlands" under Section 1.1(iii) of that agreement. The rights granted under this Section remain subject to Section 2.2 of the Real Estate Transfer Agreement.

4. Governing Law. This Assignment shall be interpreted, enforced, and governed by and under the laws of the state of California without regard to choice of law principles.

5. Integration. This Assignment constitutes the final, complete, and exclusive agreement and understanding between and among the Parties pertaining to the subject matter hereof and supersedes all prior or contemporaneous written or oral understandings, representations, warranties, arrangements and agreements between the Parties pertaining to the subject matter hereof, all of which are decreed merged into this Assignment. Notwithstanding the foregoing, except as expressly provided in Section 3 of this Assignment, the Real Estate Transfer Agreement entered into by the Parties on June 17, 2025, and its exhibits remain in full force and effect in accordance with their terms, and nothing in this Assignment limits, supersedes, releases, or merges any right or obligation arising thereunder. Assignee expressly acknowledges that it has not relied on any understandings, representations, warranties, arrangements or agreements not expressly contained in this Assignment.

ASSIGNOR'S REPRESENTATIONS

The Assignor hereby represents to Assignee, to the best of Assignor's knowledge, that Assignor:

A. has not assigned, transferred, licensed, pledged, or otherwise encumbered the Mark or Domain Name in favor of any third-party, or agreed to do any of the aforementioned;

B. is the registered holder of, or otherwise has sufficient authority and control over, the Domain Name to complete its transfer to Assignee;

C. is not aware of any pending dispute, claim, proceeding, transfer request, or other restriction affecting the ownership, registration, use, or transfer of the Domain Name;

D. has paid all registration and renewal charges currently due for the Domain Name and is not aware of any circumstance that would cause the Domain Name to expire or become unavailable before the transfer is completed;

E. the Mark or Domain Name is not and has not been the subject of or involved in any challenges, proceedings, or litigation that encumber, impact or otherwise affect their validity or use;

F. has full power and authority to enter into this Assignment and make the assignment;

G. is not aware of any violation, infringement, or misappropriation, or claim of any of these, of any third-party's rights by the Mark or Domain Name;

H. is not aware of any third-party consents, assignments or licenses that are necessary to perform under this Assignment;

I. is not aware of any fact, event, or condition that occurred or arose during the Assignor's ownership of the Mark or Domain Name that gave rise to a legal claim related to the Mark or Domain Name;

The Assignor shall immediately notify the Assignee if any facts or circumstances arise that would make any of these representations inaccurate, to the best of Assignor's knowledge and belief.

IN WITNESS WHEREOF, this Assignment is executed on the date first written above.

ASSIGNOR	ASSIGNEE
Redlands Historical Museum Association	City of Redlands
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

ATTEST:

_____
Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. I6.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Authorize the Annual Maintenance Payment to Motorola Solutions, Inc. in the amount of $126,956 for the Police Department's Spillman Computer Aided Dispatch/Records Management System (Assistant City Manager Garcia)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council authorize payment of the annual invoice for the Police Department's Spillman Computer Aided Dispatch/Records Management System to Motorola Solutions, Inc. in the amount of $126,956.

RECOMMENDATION:

City staff recommends that the City Council authorize payment of the annual invoice for the Police Department's Spillman Computer Aided Dispatch/Records Management System to Motorola Solutions, Inc. In the amount of $126,956.

DISCUSSION:

Motorola Solutions, Inc. is the vendor and owner of the software used by the Police Department for its Computer Aided Dispatch/Records Management System (CAD/RMS), also referred to as Spillman. Since the system was implemented over ten years ago, Spillman, the original developer, has provided maintenance and support to City staff through the annual maintenance agreement, which has been renewed each year since. As with many other software applications in use by the City (and is the case in all other jurisdictions for that matter), Motorola Solutions, Inc. is the only provider of software maintenance and support for the Spillman CAD/RMS system and is, as such, a sole source. Payment of the annual invoice to Motorola Solutions ensures access to routine software updates and technical support.

ALTERNATIVES:

City Council may choose not to authorize payment; however, doing so would result in the loss of software maintenance, updates, and technical support for the Police Department's CAD/RMS system.

STRATEGIC PLAN:

Not Applicable

SUBMITTED BY:
Danielle Garcia, Assistant City Manager

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Kurt Wilson, Assistant City Manager
Dana Abramovitz-Daniel, Procurement Manager
James Garland, Finance Director

PREPARED BY:
Valerie Abrego, Management Analyst

FISCAL IMPACT

Fiscal Year: 2027

Revenue Generating: No

Amount: $126,955.38

Budgeted Y/N: Yes

Account No.: 604900

Additional Appropriation Required: No

Discussion: The annual maintenance for this system totals $126,956.00. Funding for this expense was included in the FY27 budget for Management Services/DoIT.

Attachments

Motorola_Spillman_Maintenance_Support_Invoice.pdf

MOTOROLA SOLUTIONS

Need help or have question?
Scan the QR code or visit
support.motorolasolutions.com/invoicing

Motorola Solutions, Inc.
500 West Monroe
Chicago IL 60661
United States
Federal Tax ID: 36-1115800

Invoice 8230599688

Issue Date	P.O. No.	P.O. Date
Sep 01, 2026		
Contract No.	**Delivery No.**	**Customer No.**
USC000202163		

Billing Address

REDLANDS POLICE DEPT, CITY OF
ATTN: Accounts Payable
P.O. BOX 1025
REDLANDS CA 92373
United States

Shipping Address

REDLANDS POLICE DEPARTMENT
30 CAJON STREET
1270 W PARK #C
REDLANDS CA 92373
United States

Important Information

Contract Number: USC000202163-R02-JUN-26 04:29:05

For all invoice payment inquiries contact

SLT8WB@motorolasolutions.com
Telephone: 800-247-2346

Special Instructions and Comments

General Comment: Regular Invoice

Payment Details

Payment Method / Terms
Net Due in 30 Days

Payment Address
Motorola Solutions, Inc.
13108 Collections Center Drive
Chicago, IL 60693
United States

Bank
Bank of America, Dallas

Bank Account No.

ABA Routing No. for ACH

ABA Routing No. for Wire Transfer

SWIFT

Invoice Total
USD 126,955.38
Payment Due Date Oct 01, 2026

Pay Online

motorolasolutions.com/billing

Please detach here and return the bottom portion with your payment

Payment Coupon

Invoice 8230599688

Issue Date	Customer No.
Sep 01, 2026	

Please put your Transaction Number and your Customer Account Number on your payment for prompt processing.

Billing Address
REDLANDS POLICE DEPT, CITY OF
ATTN: Accounts Payable
P.O. BOX 1025
REDLANDS CA 92373
United States

Payment Address
Motorola Solutions, Inc.
13108 Collections Center Drive
Chicago, IL 60693
United States

Invoice Total
USD 126,955.38
Tax Included 0.00
Payment Due Date **Oct 01, 2026**

Provide your remittance details to:
US.remittance@motorolasolutions.com

MOTOROLA SOLUTIONS

Diversion contrary to export control law is prohibited

#	Description	Ship Date	Service Period	Unit Price	Qty	Amount
	Equipment at Site: 1862975 1011860485 30 CAJON STREET 1270 W PARK #C REDLANDS CA 92373 United States					
1	FLEX CAD MAINTENANCE (ENHANCED) - STANDARD ITEM# SSV00S00012A-SP		Oct 01, 2026 - Sep 30, 2027	2,472.13	1	2,472.13
2	FLEX NON-CUSTODIAL ARREST MAINTENANCE - STANDARD ITEM# SSV00S00396A-SP		Oct 01, 2026 - Sep 30, 2027	0.00	1	0.00
3	FLEX HUB MAINTENANCE (ENHANCED) - STANDARD ITEM# SSV00S00015A-SP		Oct 01, 2026 - Sep 30, 2027	42,088.21	1	42,088.21
4	FLEX PERSONNEL MANAGEMENT MAINTENANCE - STANDARD ITEM# SSV00S00432A-SP		Oct 01, 2026 - Sep 30, 2027	2,903.37	1	2,903.37
5	FLEX PIN MAPPING MAINTENANCE - STANDARD ITEM# SSV00S00438A-SP		Oct 01, 2026 - Sep 30, 2027	4,184.69	1	4,184.69
6	FLEX PREMISES AND HAZMAT INFORMATION MAINTENANCE - STANDARD ITEM# SSV00S00447A-SP		Oct 01, 2026 - Sep 30, 2027	1,189.04	1	1,189.04
7	FLEX SENTRYX GIS (GEOBASE) MAINTENANCE - STANDARD ITEM# SSV00S00480A-SP		Oct 01, 2026 - Sep 30, 2027	0.00	1	0.00
8	FLEX TRAFFIC INFORMATION MAINTENANCE - STANDARD ITEM# SSV00S00527A-SP		Oct 01, 2026 - Sep 30, 2027	2,058.63	1	2,058.63
9	FLEX XML ACCIDENT INTERFACE MAINTENANCE - STANDARD ITEM# SSV00S00566A-SP		Oct 01, 2026 - Sep 30, 2027	4,106.59	1	4,106.59
10	FLEX MOBILE SERVER CAD SHARE - STANDARD ITEM# SSV00S006026-SP		Oct 01, 2026 - Sep 30, 2027	14,176.11	1	14,176.11
11	FLEX TOUCH MAINTENANCE - STANDARD ITEM# SSV00S00028A-SP		Oct 01, 2026 - Sep 30, 2027	1,886.48	1	1,886.48
12	FLEX E9-1-1 INTERFACE MAINTENANCE - STANDARD ITEM# SSV00S00181A-SP		Oct 01, 2026 - Sep 30, 2027	2,472.13	1	2,472.13
13	FLEX LAW RECORDS MAINTENANCE - STANDARD ITEM# SSV00S00033A-SP		Oct 01, 2026 - Sep 30, 2027	1,945.04	1	1,945.04
14	FLEX MOBILE AVL AND MAPPING MAINTENANCE - STANDARD ITEM# SSV00S00036A-SP		Oct 01, 2026 - Sep 30, 2027	9,673.76	1	9,673.76
15	FLEX MOBILE RECORDS MAINTENANCE - STANDARD ITEM# SSV00S00038A-SP		Oct 01, 2026 - Sep 30, 2027	2,903.37	1	2,903.37
16	FLEX STATELINK MAINTENANCE - STANDARD ITEM# SSV00S00052A-SP		Oct 01, 2026 - Sep 30, 2027	4,848.42	1	4,848.42
17	FLEX CAD MAPPING MAINTENANCE -		Oct 01, 2026 - Sep 30, 2027	5,148.33	1	5,148.33

MOTOROLA SOLUTIONS

#	Description	Ship Date	Service Period	Unit Price	Qty	Amount
	STANDARD ITEM# SSV00S00072A-SP					
18	FLEX DATA WAREHOUSE INTERFACE MAINTENANCE - STANDARD ITEM# SSV00S00164A-SP		Oct 01, 2026 - Sep 30, 2027	0.00	1	0.00
19	FLEX IBR MAINTENANCE - STANDARD ITEM# SSV00S00050A-SP		Oct 01, 2026 - Sep 30, 2027	2,417.72	1	2,417.72
20	FLEX EQUIPMENT MAINTENANCE MAINTENANCE - STANDARD ITEM# SSV00S00184A-SP		Oct 01, 2026 - Sep 30, 2027	0.00	1	0.00
21	FLEX IMAGING MAINTENANCE - STANDARD ITEM# SSV00S00262A-SP		Oct 01, 2026 - Sep 30, 2027	6,954.94	1	6,954.94
22	FLEX LICENSES AND PERMITS MAINTENANCE - STANDARD ITEM# SSV00S00301A-SP		Oct 01, 2026 - Sep 30, 2027	1,189.04	1	1,189.04
23	FLEX MOBILE ARREST FORM MAINTENANCE - STANDARD ITEM# SSV00S00331A-SP		Oct 01, 2026 - Sep 30, 2027	4,692.02	1	4,692.02
24	FLEX MOBILE FIELD REPORT WITH FIELD INTERVIEW MAINTENANCE - STANDARD ITEM# SSV00S00334A-SP		Oct 01, 2026 - Sep 30, 2027	3,655.83	1	3,655.83
25	FLEX MOBILE STATE & NATIONAL QUERIES MAINTENANCE - STANDARD ITEM# SSV00S00352A-SP		Oct 01, 2026 - Sep 30, 2027	960.11	1	960.11
26	FLEX MOBILE VOICELESS CAD MAINTENANCE - STANDARD ITEM# SSV00S00354A-SP		Oct 01, 2026 - Sep 30, 2027	5,029.42	1	5,029.42
			Site: CA Tax at 0%			0.00
			Site Total			126,955.38

USD Subtotal	126,955.38
USD Total Tax	0.00
USD Invoice Total	**126,955.38**
USD Amount Due	126,955.38

Disclaimer:

There are certain telecommunications-regulated services provided for under the Regulated Services Addendum ("RSA") and may be billed to customers in this invoice provided by Motorola Solutions, Inc.'s wholly-owned subsidiary, Motorola Solutions Connectivity, Inc. ("MSCI"). If you receive any of these services under the RSA, such services are billed by Motorola Solutions, Inc. on MSCI's behalf. This applies solely to services delineated in and provided under the RSA.

If you have any questions as to individual services, please do not hesitate to reach out to your Motorola Solutions representative.

City Council **AGENDA ITEM NO. I7.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve an Intergovernmental Purchase of Dell Computers and Accessories for a Citywide Computer Refresh in the amount of $130,206 (Assistant City Manager Garcia)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council approve the intergovernmental purchase of Dell computers and accessories for a citywide computer refresh in the amount of $130,206.

RECOMMENDATION:

Staff recommends that the City Council approve the intergovernmental purchase of Dell computers and accessories for a citywide computer refresh in the amount of $130,206.

DISCUSSION:

The City of Redlands' Division of Innovation and Technology (DoIT) is working toward establishing a consistent and standardized technology refresh cycle for end-user computing equipment. The goal of this policy is to ensure that the City's technology assets remain secure, reliable, supported, and capable of meeting operational requirements. This policy will apply to all computing hardware assigned to City employees, Police Department personnel, training environments, and other authorized users. This policy aims to set a standard five-year refresh cycle for all City and Police Department desktops and laptops.

After assessing the City's current computing inventory, DoIT has identified 92 desktops and 38 laptops that are at end of life, and an additional 153 desktops and 5 laptops set to reach end of life during this fiscal year. Based on that assessment, DoIT is proposing two purchases of Dell computers during this fiscal year. Separating the hardware refresh into two purchases will reduce storage time and maximize included warranty coverage.

The first purchase, presented here, calls for the City to procure 50 desktops and 22 laptops, as well as associated accessories, from Dell Technologies. The purchased hardware will go towards the immediate replacement of identified end of life units and also allows for the consolidation of City resources for those employees that were utilizing a desktop and a laptop. Those employees will convert to using a single laptop with a docking station. Ultimately, the targeted replacement of these end of life units will preempt expensive maintenance and downtime and allow City staff to utilize equipment more efficiently.

Staff followed the City's procurement guidelines by examining and selecting an existing competitively-bid cooperative contract with the National Association of State Procurement Officials (NASPO) ValuePoint. NASPO is a non-profit association made up of the directors of the central purchasing offices of the 50 states, the District of Columbia, and territories of the United States. By utilizing the NASPO ValuePoint cooperative purchasing program, the City is able to benefit from the combined purchasing power of more than 50,000 government, education, and non-profit organizations. The purpose of these cooperative contract programs enable the City to take advantage of preferred pricing and administrative efficiencies. Based on staff's assessment, the new computer hardware proposed for purchase are recommended to be sourced through this cooperative purchasing agreement.

ALTERNATIVES:

City Council may choose to reject, modify, or table the proposed purchase.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Danielle Garcia, Assistant City Manager

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Kurt Wilson, Assistant City Manager
James Garland, Finance Director
Dana Abramovitz-Daniel, Procurement Manager
James Garland, Finance Director

PREPARED BY:
Valerie Abrego, Management Analyst

FISCAL IMPACT

Fiscal Year: 2027

Revenue Generating: No

Amount: $130,206

Budgeted Y/N: Yes

Account No.: 604900

Additional Appropriation Required: No

Discussion: Funding for this purchase is included in the IT Divisions' budget for FY27.

Attachments

Intergovernmental_Request_Form-_Dell-Workstation_Refresh.pdf
NASPO_CA_Participating_Addendum.pdf
NASPO_Master_Agreement.pdf
Dell_Hardware_Quote.pdf

Intergovernmental/ Piggyback Contract Use Request

(Attach to PR form)

The Management Services-DoIT Department requests the purchase of the following item(s) from:

Original Contracting Entity: Minnesota National Association of State Procurement Officials (NASPO)
Contract#: C000001115143 Minnesota NASPO ValuePoint Master Agreement # 23026 California Participating Addendum Number 7-23-70-55-01
Contract Term: July 14th, 2023- June 30th, 2027
Method of original contract award: ☑ Competitive ☐ Non-Competitive, based on: ☐Preferred source ☐Sole ☐Single source ☐Emergency ☐Other:
Does the original contract contain language contemplating contract extension to additional users? ☑Yes ☐ No

Please attach: vendor agreement to sale to the City AND Entity agreement/contract language allowing Piggyback

Description of Product/Service intend to acquire	Unit Price	Total
Qty. 50-Dell Pro Slim Plus QBS1250	$ 1,535.07	$ 76,753.50
Qty. 22- Dell PRO 5 16 P516260	$ 1,923.75	$ 42,322.50
Qty. 10- Dell Pro Thunderbolt 4 Dock WD25TB4	$ 209.99	$ 2,099.90
Environmental Fee		$ 110.00
Tax	$ 8,919.84	
	Grand Total	$ 130,205.74

Vendor:	Dell Technologies
Contact:	KC Dudley
Address 1:	One Dell Way
Address 2:	Mail Stop 8129
City/State/Zip:	Round Rock, TX 78682
Telephone:	800-456-3355
Fax:	
Web/E-Mail:	kc.dudley@dell.com

Delivery/Service Location	
Contact:	Eric OWens
Telephone:	909-355-4775
Department:	Management Services
Address 1:	35 Cajon St., Suite 30
Address 2:	Redlands, CA 92373
Additional Comments	

Purchasing Agent Approval: _____ Date: _____

City Manager Approval: _____ Date: _____

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-23-70-55-01
AMENDMENT 3

Computer Equipment, Peripherals & Related Services
Minnesota NASPO ValuePoint Master Agreement Number 23026
Dell Marketing L.P. (Contractor)

The parties mutually agree to amend Participating Addendum 7-23-70-55-01 as follows:

1) Agreement is extended from June 30, 2026, to June 30, 2027. **Section 2. TERM, subparagraph A** is revised to read as follows:

   A. The term of this Participating Addendum shall begin upon signature approval by the State and will end June 30, 2027, or upon termination by the State, whichever occurs first.

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Participating Addendum as of the date of execution by both parties below.

STATE OF CALIFORNIA	**CONTRACTOR**
Department of General Services	Dell Marketing L.P.
Agency Name	*Contractor Name*
Julie Matthews Digitally signed by Julie Matthews Date: 2026.05.12 16:50:58 -07'00' 5/12/2026	Ana Pitti Ana Pitti (May 7, 2026 17:29:26 CDT) May 7, 2026
Authorized Signature *Date Signed*	*Authorized Signature* *Date Signed*
Julie Matthews, MAU2 Supervisor	Ana Pitti | Paralegal Senior Analyst
Printed Name/Title of Person Signing	*Printed Name/Title of Person Signing*
707 Third Street West Sacramento, CA 95605	One Dell Way Round Rock, TX 78682
Address	*Address*

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-23-70-55-01
AMENDMENT 2

Computer Equipment, Peripherals & Related Services
Minnesota NASPO ValuePoint Master Agreement Number 23026
Dell Marketing L.P. (Contractor)

The parties mutually agree to amend Participating Addendum 7-23-70-55-01 as follows:

1) Agreement is extended from June 30, 2025, to June 30, 2026. **Section 2. TERM, subparagraph A** is revised to read as follows:

   A. The term of this Participating Addendum shall begin upon signature approval by the State and will end June 30, 2026, or upon termination by the State, whichever occurs first.

2) **Section 22. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING** is hereby deleted and replaced with the following:

22. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI)

DEFINITIONS:

For purposes of this Section, the following terms shall be given the meaning shown below. Capitalized terms used below and not defined in this Section shall have the meaning set forth in Section 1 (Definitions) or in the text of the IT General Provisions (rev. 06/21/2022).

Artificial Intelligence (AI): an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments (Gov Code §§ 11549.64 & 11546.45.5).

GenAI Training Data: any content, information, or data that is used to train, tune, test, or validate a GenAI, including text, images, video, audio, code, or similar types of input.

Generated Data: any output, results, content, or other data that is produced by GenAI, including but not limited to text, images, video, audio, code, or similar types of output.

Generative AI (GenAI): an AI system that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's GenAI Training Data (Gov Code §11549.64).

Hallucination: Generated Data that is nonsensical, false, or misleading, and is not based on real or existing data, but is instead produced by bias or the GenAI's extrapolation or creative interpretation of its Gen AI Training Data.

Materially Impacts: shall have the same meaning set forth in State Administrative Manual (SAM) 4986.2.

Prompt: any written, spoken, or rendered information provided as a query, command, or other form of input, to any GenAI in connection with this Contract. For avoidance of doubt, Prompt includes any input automatically detected or created by the GenAI, as well as any derivate works of a Prompt or collection of Prompts.

GENAI DISCLOSURE OBLIGATIONS:

Disclosure Obligations:

a) Contractor must immediately notify the State in writing if it: (1) intends to provide GenAI as a Deliverable to the State; or (2) intends to utilize GenAI, including GenAI from third parties, to complete all or a portion of any Deliverable that materially impacts: (i) functionality of the System, (ii) risk to the State, or (iii) Contract performance. For avoidance of doubt, the term "materially impacts" shall have the same meaning set forth in State Administrative Manual (SAM) § 4986.2 Definitions for GenAI.
b) Such notification shall be provided to the State designee identified in this Contract.
c) At the direction of the State, Contractor shall discontinue the provision to the State of any previously unreported GenAI that results in a material impact to the functionality of the System, risk to the State, or Contract performance, as determined by the State.
d) If the use of previously undisclosed GenAI is approved by the State, then Contractor will update the Deliverable description, and the Parties will amend the Contract accordingly, which may include incorporating the GenAI Special Provisions into the Contract, at no additional cost to the State.

Failure to Disclose or Discontinue GenAI Use: The State, at its sole discretion, may consider Contractor's failure to disclose or discontinue the provision or use of GenAI as described above, to constitute a material breach of Contract when such failure results in a material impact to functionality of the System, risk to the State, or Contract performance. The State is entitled to seek any and all remedies available to it under law as a result of such breach, including but not limited to termination of the contract, for default pursuant to Section 23 (Termination for Default) of the IT General Provisions (rev. 06/21/2022).

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Participating Addendum as of the date of execution by both parties below.

STATE OF CALIFORNIA	**CONTRACTOR**
Department of General Services	Dell Marketing L.P.
Agency Name	*Contractor Name*
Julie Matthews Digitally signed by Julie Matthews Date: 2025.05.15 17:06:00 -07'00' — 5/15/2025	Ana Pitti — May 5, 2025
Authorized Signature — *Date Signed*	*Authorized Signature* — *Date Signed*
Julie Matthews, MAU2 Supervisor	Ana Pitti | Paralegal Senior Analyst
Printed Name/Title of Person Signing	*Printed Name/Title of Person Signing*
707 Third Street West Sacramento, CA 95605	One Dell Way Round Rock, TX 78682
Address	*Address*

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-23-70-55-01
AMENDMENT 1

Computer Equipment, Peripherals & Related Services
Minnesota NASPO ValuePoint Master Agreement Number 23026
Dell Marketing L.P. (Contractor)

The parties mutually agree to amend Participating Addendum 7-23-70-55-01 as follows:

1) **Section 22. GENERATIVE ARTIFIFICAL INTELLIGENCE (GENAI) REPORTING** is hereby added to read as follows:

22. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING

The State of California seeks to realize the potential benefits of GenAI, through the development and deployment of GenAI tools, while balancing the risks of these new technologies.

Upon request by an ordering agency, Contractor must complete a GenAI Reporting and Fact Sheet (STD 1000) to identify if their solution or service includes, or makes available, any GenAI including, GenAI from third parties or subcontractors.

During the term of the contract, Contractor must notify the State in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000) to notify the State of any new or previously unreported GenAI technology.

At the direction of the State, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk or contract performance, until use of such GenAI technology has been approved by the State.

Failure to disclose GenAI use to the State and submit the GenAI Reporting and Factsheet (STD 1000) may be considered a breach of the contract by the State at its sole discretion and the State may consider such failure to disclose GenAI and/or failure to submit the GenAI Reporting and Factsheet (STD 1000) as grounds for the immediate termination of the contract. The State is entitled to seek any and all relief to which it may be entitled to as a result of such non-disclosure.

The State reserves the right to amend the contract, without additional cost, to incorporate GenAI Special Provisions into the contract at its sole discretion and/or terminate any contract that presents an unacceptable level of risk to the State.

If Contractor identifies GenAI in their solution, a copy of the STD 1000 must be submitted to the DGS State Contract Administrator.

All other terms and conditions of the Participating Addendum shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Participating Addendum as of the date of execution by both parties below.

STATE OF CALIFORNIA	**CONTRACTOR**
Department of General Services	Dell Marketing L.P.
Agency Name	*Contractor Name*
Julie Matthews Digitally signed by Julie Matthews Date: 2024.10.25 17:34:21 -07'00' — 10/25/2024	Katherine_Castillo1 Digitally signed by Katherine_Castillo1 Date: 2024.08.23 15:42:23 -05'00'
Authorized Signature — *Date Signed*	*Authorized Signature* — *Date Signed*
Julie Matthews, MAU2 Supervisor	Katherine Castillo/Paralegal Advisor
Printed Name/Title of Person Signing	*Printed Name/Title of Person Signing*
707 Third Street West Sacramento, CA 95605	One Dell Way Round Rock, TX 78682
Address	*Address*

STATE OF CALIFORNIA
PARTICIPATING ADDENDUM NUMBER 7-23-70-55-01

Computer Equipment, Peripherals & Related Services
Minnesota NASPO ValuePoint Master Agreement Number 23026
Dell Marketing L.P. (Contractor)

This Participating Addendum Number 7-23-70-55-01 is entered into between the State of California, Department of General Services (hereafter referred to as "State" or "DGS") and Dell Marketing L.P. (hereafter referred to as "Contractor") under the lead state of Minnesota NASPO ValuePoint Master Agreement Number 23026.

1. SCOPE

A. This Participating Addendum covers the purchase of computer equipment (desktops, laptops, tablets, servers, and storage, including related peripherals & services) under the Minnesota NASPO ValuePoint Master Agreement. The Minnesota NASPO ValuePoint Master Agreement is hereby incorporated by reference. Product/service categories included under this Participating Addendum are identified in Section 5 (Available Products and Services).

B. This Participating Addendum is available for use by California state agencies and local governments. A local government is defined as any city, county, city and county, district, or other local governmental body, school district or corporation empowered to expend public funds. The State Agency Listing (https://www.ca.gov/agenciesall/) provides a comprehensive list of state agencies.

C. Each local government is to make its own determination whether this Participating Addendum and the Minnesota NASPO ValuePoint Master Agreement are consistent with its procurement policies and regulations.

2. TERM

A. The term of this Participating Addendum shall begin February 1, 2024, or upon signature approval by the State whichever occurs later, and will end June 30, 2025, or upon termination by the State, whichever occurs first.

B. Lead state amendments to extend the NASPO ValuePoint Master Agreement term date are not automatically incorporated into this Participating Addendum. Extension(s) to the term of this Participating Addendum will be through a written amendment upon mutual agreement between the State and the Contractor.

C. Order placement and execution shall be on or before the expiration of this Participating Addendum. However, delivery of products or completion of services may be up to 120 days after the Participating Addendum expiration date.

3. TERMS AND CONDITIONS/INCORPORATION OF DOCUMENTS

A. Terms and conditions listed below are hereby incorporated by reference and made a part of this Participating Addendum as if attached herein and shall apply to the purchase of goods or services made under this Participating Addendum.

1) General Provisions – Information Technology (GSPD-401IT) effective 6/21/2022

B. Terms can be viewed on the DGS Procurement Division website (https://www.dgs.ca.gov/PD/Resources/Page-Content/Procurement-Division-Resources-List-Folder/Required-Language-for-Solicitations-and-Contracts).

4. ORDER OF PRECEDENCE

A. In the event of any inconsistency between the articles, attachments, or provisions which constitute this agreement, the following descending order of precedence shall apply:

1) California Participating Addendum Number 7-23-70-55-01
2) Minnesota NASPO ValuePoint Master Agreement Number 23026

5. AVAILABLE PRODUCTS AND SERVICES

A. The following product and service offerings from the Minnesota NASPO ValuePoint Master Agreement Number 23026 are allowed under this Participating Addendum:

1) Band 1, Personal Computing Devices – Windows Operating Systems: Desktops, Laptops, Tablets
2) Band 2, Personal Computing Devices – Non-Windows Operating Systems: Desktops, Laptops, Tablets
3) Band 3, Servers and Storage

6. RESTRICTIONS/DISALLOWED PRODUCTS AND SERVICES

A. Configuration limits: The dollar limits identified below are based on a SINGLE computer/system configuration. This is NOT a restriction on the purchase of multiple configurations (e.g., an entity could purchase 10 laptops at $15,000 each, for a total purchase price of $150,000).

ITEM	CONFIGURATION
Band 1	$15,000
Band 2	$15,000
Band 3	$1,000,000
Peripherals	$10,000
Services	Addressed in the customer specific Purchase Orders

B. Services must be related to the procurement of equipment.

C. The following restrictions apply to state agency purchases under this Participating Addendum:

1) Product and service categories that are available on mandatory California statewide contracts cannot be purchased from this Participating Addendum by state agencies without an exemption. State agencies are responsible for obtaining a mandatory statewide contract exemption from DGS prior to issuing a purchase order.

2) Service-only purchases are disallowed. (Exception: Equipment maintenance service purchases are allowed).

3) Services that fall within the definition of “public works” as defined in Public Contract Code section 1101 and Labor Code section 1720 are disallowed under this Participating Addendum and must be procured by alternate means. This restriction is not applicable to local governments.

4) Leasing/rental is not allowed.

5) Professional services are not allowed.

6) Cloud services are not allowed.

7. PRICING

A. Contractor’s pricing is outlined in the Minnesota NASPO ValuePoint Master Agreement Number 23026.

B. Contractor shall notify the State Contract Administrator of any amendments and pricing adjustments approved and executed by the state of Minnesota.

8. AUTHORIZED RESELLERS

A. Contractor may use State-approved Authorized Resellers under this Participating Addendum for sales and service functions as defined herein.

1) Authorized Resellers must accept purchase orders and accept payment from ordering agencies for products and services offered under this Participating Addendum.

2) Authorized Resellers are responsible for sending a copy of all purchase orders and invoices to the Contractor for compliance with quarterly usage reporting and administrative fee requirements.

3) All purchase documents to Authorized Resellers shall reference the Participating Addendum Number and Contractor Name.

B. Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions under this Participating Addendum, even if work is performed by Authorized Resellers. All State policies, guidelines, and requirements shall apply to Authorized Resellers.

C. Contractor will be the sole point of contact with regard to Participating Addendum contractual matters, reporting, and administrative fee requirements.

D. Subject to the approval of the State, Authorized Resellers may be added on a quarterly basis during the term of the Participating Addendum. Contractors shall notify the State in writing of any deleted Authorized Resellers or changes to current Authorized Resellers' information at any time.

E. Contractor will be required to submit Authorized Reseller requests, in a format specified by the State, to the State Contract Administrator for approval.

F. State-approved Authorized Resellers will be posted on the State's Cal eProcure website.

9. SUBCONTRACTORS

A. Nothing contained in this Participating Addendum or otherwise, shall create any contractual relation between the State and any subcontractors, and no subcontract shall relieve Contractor of its responsibilities and obligations hereunder. Contractor agrees to be as fully responsible to the State for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by the Contractor. Contractor's obligation to pay its subcontractors is an independent obligation from the State's obligation to make payments to the Contractor.

B. Contractor shall perform the work contemplated with resources available within its own organization and no portion of the work shall be subcontracted except for subcontractors listed on the Bidder Declaration (GSPD-05-105) provided to ordering agencies at the time an order is quoted.

C. As the prime Contractor, Contractor is responsible for reports and fees required by the terms and conditions of the NASPO ValuePoint Master Agreement and Participating Addendum.

D. Any subcontract in excess of $25,000, entered into as a result of this Participating Addendum, shall contain all the provisions stipulated in this Participating Addendum to be applicable to subcontractors.

10. ORDERING AGENCY RESPONSIBILITIES

A. State agency and local government use of this Participating Addendum is optional.

B. State agencies and local governments must follow the ordering procedures outlined within the User Instructions guide, administered by the State Contract Administrator, to execute orders against this Participating Addendum. User Instructions are posted on the State's Cal eProcure website.

C. All purchase orders executed under this Participating Addendum shall include the Participating Addendum Number 7-23-70-55-01.

11. STATE AGENCY BUY RECYCLED CAMPAIGN (SABRC)

A. State agencies are required to report purchases made within the eleven product categories in the California Department of Resources Recycling and Recovery's State Agency Buy Recycled Campaign (SABRC) per Public Contract Code sections 12200-12217.

B. Contractor will be required to complete and return a Postconsumer Recycled-Content Certification form (https://calrecycle.ca.gov/buyrecycled/stateagency/vendored/form74guide/) upon request by the state agency.

12. DELIVERY

A. Delivery shall occur within 30 days after receipt of order, or as negotiated between ordering agency and Contractor and included in the purchase order, or as otherwise stipulated in the NASPO ValuePoint Master Agreement.

B. Free On Board (F.O.B.) Destination, freight prepaid by the Contractor, to the ordering agency's receiving point.

13. INVOICING AND PAYMENT

A. Payment will be made in accordance with IT General Provisions Paragraph 30 (Required Payment Date).

B. Invoices shall be sent to the address identified in the ordering agency's purchase order. The Participating Addendum Number and ordering agency purchase order number shall appear on each invoice for all purchases placed under this Participating Addendum.

C. Contractor does not accept the State of California credit card (CAL-Card) for payment of invoices.

14. USAGE REPORTING

A. Contractor shall submit usage reports on a quarterly basis to the State Contract Administrator for all California entity purchases using the report template attached hereto as Attachment A. The report is due even when there is no activity.

B. The State Contract Administrator reserves the right to modify Attachment A and require Contractor to provide additional order information during the course of this Participating Addendum.

C. The report shall be an Excel spreadsheet transmitted electronically to the DGS Cooperatives mailbox (PDCooperatives@dgs.ca.gov).

D. Any report that does not follow the required format or that excludes information will be deemed incomplete. Contractor will be responsible for submitting corrected reports within five (5) business days of the date of written notification from the State.

E. Tax must not be included in the report, even if it is on the purchase order.

F. Reports are due for each quarter as follows:

Reporting Period	Due Date
January 1 to March 31	April 30
April 1 to June 30	July 31
July 1 to September 30	October 31
October 1 to December 31	January 31

G. Failure to meet reporting requirements and submit the reports on a timely basis shall constitute grounds for suspension of this Participating Addendum.

H. Time extensions may be approved only if all due reports have been submitted to the State.

15. ADMINISTRATIVE FEE

A. Contractor is required to remit to DGS an administrative fee amount equal to 1.25% of the sales for the quarterly reporting period less freight, taxes, returned products and credits. (For example, if the net sales for the reporting quarter totals $100,000.00, the incentive fee due to DGS would be $1,250.00.)

B. The administrative fee shall not be included as an adjustment to Contractor's NASPO ValuePoint Master Agreement pricing.

C. The administrative fee shall not be invoiced or charged to the ordering agency.

D. Payment of the administrative fee is due irrespective of payment status from ordering agencies.

E. Payment may be made in the form of an electronic payment using the LPA Payment Portal website (https://www.dgs.ca.gov/PD/Services/Page-Content/Procurement-Division-Services-List-Folder/Access-LPA-Payment-Portal) or by submitting a check payable to the State of California, Department of General Services.

F. Administrative fee payments made by check must include the Participating Addendum Number on the check and be submitted to the following address:

Department of General Services
Procurement Division
Attn: MAPS Payment Processing
707 Third Street, 2nd Floor
West Sacramento, CA 95605

G. Administrative fee payments are due for each quarter as follows:

Reporting Period	Due Date
January 1 to March 31	April 30
April 1 to June 30	July 31
July 1 to September 30	October 31
October 1 to December 31	January 31

H. Failure to meet administrative fee requirements and submit fees on a timely basis shall constitute grounds for suspension of this Participating Addendum.

16. CONTRACT MANAGEMENT

A. The primary Contractor Contract Manager for this Participating Addendum shall be as follows:

Contractor	Contract Manager
Name:	Ashley Salinas
Phone:	(512) 542-1237
Fax:	n/a
Email	A.Salinas@dell.com
Address:	Dell Marketing L.P. Attn: Ashley Salinas One Dell Way Round Rock, TX 78682

B. The State Contract Administrator for this Participating Addendum shall be as follows:

State	Contract Administrator
Name:	Katelynne Leisenring
Phone:	(279) 946-8129
Email	katelynne.leisenring@dgs.ca.gov
Address:	State of California Department of General Services Procurement Division 707 Third Street, 2nd Floor, MS 2-202 West Sacramento, CA 95605

C. Should the contact information for either party change, the party will provide written notice with updated information no later than ten (10) business days after the change.

17. TERMINATION OF AGREEMENT

The State may terminate this Participating Addendum at any time upon 30 days prior written notice to the Contractor. Upon termination or other expiration of this Participating Addendum, each party will assist the other party in orderly termination of the Participating Addendum and the transfer of all assets, tangible, and intangible, as may facilitate the orderly, non-disrupted business continuation of each party. This provision shall not relieve the Contractor of the obligation to perform under any purchase order or other similar ordering document executed prior to the termination becoming effective.

18. AMENDMENT

No amendment or variation of the terms of this Participating Addendum shall be valid unless made in writing, signed by the parties, and approved as required. No oral understanding or agreement not incorporated in the Participating Addendum is binding on any of the parties.

19. NEWS RELEASES

Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this Participating Addendum shall not be made without prior written approval from the State.

20. EXECUTIVE ORDER N-6-22 – RUSSIA SANCTIONS

On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. “Economic Sanctions” refers to sanctions imposed by the U.S. government in response to Russia’s actions in Ukraine, as well as any sanctions imposed under state law. The EO directs state agencies to terminate contracts with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that shall be grounds for termination of this Participating Addendum. The State shall provide Contractor advance written notice of such termination, allowing Contractor at least thirty (30) calendar days to provide a written response. Termination shall be at the sole discretion of the State.

21. AGREEMENT

A. This Participating Addendum and the Master Agreement together with its exhibits and/or amendments, set forth the entire agreement between the parties with respect to the subject matter of all previous communications, representations, or agreements, whether oral or written, with respect to the subject matter hereof. Terms and conditions inconsistent with, contrary or in addition to the terms and conditions of this Participating Addendum and the Master Agreement, together with its exhibits and/or amendments, shall not be added to or incorporated into this Participating Addendum or the Master Agreement and its exhibits and/or amendments, by any subsequent purchase order or otherwise, and any such attempts to add or incorporate such terms and conditions are hereby rejected. The terms and conditions of this Participating Addendum and the Master Agreement and its exhibits and/or amendments shall prevail and govern in the case of any such inconsistent or additional terms.

B. By signing this Participating Addendum, Contractor agrees to offer the same products/services available on the Minnesota NASPO ValuePoint Master Agreement Number 23026, at prices equal to or lower than the prices on that agreement.

IN WITNESS WHEREOF, the parties have executed this Participating Addendum as of the date of execution by both parties below.

STATE OF CALIFORNIA		**CONTRACTOR**	
Department of General Services		Dell Marketing L.P.	
Agency Name		*Contractor Name*	
Julie Matthews Digitally signed by Julie Matthews Date: 2024.01.23 13:54:09 -08'00'	1/23/2024	Katherine Castillo	01/22/2024
Authorized Signature	*Date Signed*	*Authorized Signature*	*Date Signed*
Julie Matthews, MAU2 Supervisor		Katherine Castillo- Paralegal Advisor	
Printed Name/Title of Person Signing		*Printed Name/Title of Person Signing*	
707 Third Street West Sacramento, CA 95605		One Dell Way Round Rock, TX 78682	
Address		*Address*	

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

ASSIGNMENT OF NASPO MASTER AGREEMENT 23004

This Assignment Agreement is by and among the State of Minnesota, acting through its Commissioner of Administration (State), Dell Inc., One Dell Way, Round Rock, TX 78682 (Original Contractor), and Dell Marketing L.P., One Dell Way, Mailstop RR1-33 Legal, Round Rock, TX 78682 (Assigned Contractor).

WHEREAS, the State has an agreement with the Original Contractor identified as Contract 23004, effective July 14, 2023, through June 30, 2025 (Contract), to provide Computer Equipment, Peripherals & Related Services; and

WHEREAS, the Original Contractor wishes to assign all its interests in the Contract to the Assigned Contractor; and

WHEREAS, the assignment provision of the Contract provides assignment of the agreement only upon written consent of the State.

NOW, THEREFORE, it is agreed by the parties to amend the Contract as follows:

1. The Assigned Contractor is assigned Contract 23026 to accommodate participating addenda under the Master Agreement.

2. This Assignment Agreement will become effective upon its approval and execution by the parties and approval of the appropriate State officials, pursuant to Minn. Stat. § 16C.05, subd. 2.

3. The State hereby approves the request of the Original Contractor to assign the Assigned Contractor all its interests, rights, and responsibilities, duties, and other provisions set forth in the Contract, which is attached and incorporated as Exhibit A, provided the Original Contractor and the Assigned Contractor agree to all provisions set forth in this Assignment Agreement.

4. Representations and Warranties:

    a. The Original Contractor represents and warrants to the State that it is not in default of any of its obligations under the Contract.

    b. The Assigned Contractor represents and warrants to the State that: (i) as of the effective date of this Assignment Agreement, the Assigned Contractor will have received sufficient information, right to technology, and key personnel sufficient to properly perform the duties, responsibilities, obligations, and all other provisions assigned to it, and (ii) the Assigned Contractor is ready, willing, and able to perform all of the duties, obligations, and responsibilities of the Contract.

    c. The representations and warranties set forth in this Section 4 are for the sole benefit of the State and its permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other person or entity (including the Original Contractor and the Assigned Contractor) any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Assignment Agreement.

5. The Assigned Contractor accepts assignment of all of the provisions of the Contract.

6. Any and all amounts due to the Original Contractor by a Participating Entity for goods or services provided by the Original Contractor prior to July 14, 2023, under the Contract will be paid to the Original Contractor by the Participating Entity. Any and all amounts due under the Contract on or after July 14, 2023, will be paid to the Assigned Contractor by the Participating Entity and the Original Contractor.

7. When applicable, payment for remaining work and travel expenses from the Contract will be paid at the rates set in the Contract. The amount to be paid to the Assigned Contractor will not exceed the Contract's total costs, minus the

total payments made to the Original Contractor.

8. If applicable, the Assigned Contractor will provide proof of insurance with the coverage and in the amounts called for in the original solicitation document, attached herein.

9. If applicable, the Assigned Contractor will provide a copy of its Affirmative Action Certification as approved by the Minnesota Department of Human Rights.

10. If applicable, the Assigned Contractor will provide a copy of its Equal Pay Certification as approved by the Minnesota Department of Human Rights.

This Assignment Agreement is effective upon the date that the final required signatures are obtained.

IN WITNESS WHEREOF, the parties have caused this Assignment Agreement to be duly executed intending to be bound thereby.

1. ORIGINAL CONTRACTOR

Dell Inc.

The Original Contract Vendor certifies that the appropriate person(s) have executed this document on behalf of the Contract Vendor as required by applicable articles, bylaws, resolutions, or ordinances.

By: DocuSigned by: Christopher Alan Garcia
Signature ECE99192885E4FE...

Christopher Alan Garcia
Printed Name

Title: Asst. Corp Secretary & SVP Legal

Date: 9/7/2023

By: _____

Title: _____

Date: _____

2. ASSIGNED CONTRACTOR

Dell Marketing L.P.

The Assigned Contract Vendor certifies that the appropriate person(s) have executed the Contract on behalf of the Contract Vendor as required by applicable articles, bylaws, resolutions, or ordinances.

By: DocuSigned by: Katherine Castillo
Signature 8DEF23302D0B4B8...

Katherine Castillo
Printed Name

Title: ParaLegal Advisor

Date: 9/7/2023

By: _____

Title: _____

Date: _____

3. OFFICE OF STATE PROCUREMENT

In accordance with Minn. Stat. §16C.03, Subd. 3.

By: DocuSigned by: Elizabeth M. Randa
Signature 742DE739C8ED492...

Elizabeth M. Randa
Printed Name

Title: Acquisition Management Specialist

Date: 9/7/2023

4. COMMISSIONER OF ADMINISTRATION

Or delegated representative.

By: DocuSigned by: Andy Doran
Signature 68D02A26D7604BA...

Andy Doran
Printed Name

Title: IT Acquisitions Supervisor

Date: 9/7/2023

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

EXHIBIT A: CONTRACT

Attached and incorporated into Exhibit A is the following document(s):

- NASPO Master Agreement 23004.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

NASPO ValuePoint Master Agreement No.: 23004

This Contract is between the State of Minnesota, acting through its Commissioner of Administration ("Lead State") and Dell Inc., whose designated business address is One Dell Way, Round Rock, TX 78682 ("Contractor"). State and Contractor may be referred to jointly as "Parties."

Recitals

1. The State of Minnesota, Department of Administration, Office of State Procurement, on behalf of the State of Minnesota and NASPO ValuePoint Cooperative Procurement Program ("NASPO ValuePoint") issued a solicitation to establish Minnesota NASPO ValuePoint Master Agreement(s) ("Contract") with qualified manufacturers for Computer Equipment (Desktops, Laptops, Tablets, Servers, and Storage, including related Peripherals & Services);

2. Contractor provided a response to the Solicitation indicating its interest in and ability to provide the goods or services requested in the Solicitation; and

3. Subsequent to an evaluation in accordance with the terms of the Solicitation and negotiation, the Parties desire to enter into a contract; and

4. All authorized governmental entities in any state or participating US Territory are welcome to use the resulting Master Agreement through NASPO ValuePoint with the approval of the State Chief Procurement Official. Upon final award of the overarching Master Agreement, Contractors are able to sign Participating Addendums (PA) at the option of Participating States. Participating States reserve the right to add state specific terms and conditions and modify the scope of the contract in their Participating Addendum as allowed by the Master Agreement.

Accordingly, the Parties agree as follows:

Contract

1. **Term of Contract**

a. Effective date. July 1, 2023, or the date the Lead State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later.

b. Expiration date. June 30, 2025. This Master Agreement may be extended for up to an additional 36 months, in increments as determined by the Lead State, through a duly executed amendment.

c. If, in the judgment of the Lead State, a follow-on, competitive procurement will be unavoidably delayed beyond the planned date of execution of the follow-on master agreement, this Master Agreement may be extended for a reasonable period of time, not to exceed six months. This subsection shall not be deemed to limit the authority of a Lead State under its state law otherwise to negotiate contract extensions.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

2. **Representations and Warranties**

a. Under Minn. Stat. §§ 15.061 and 16C.03, subd. 3, and other applicable law the Lead State is empowered to engage such assistance as deemed necessary.

b. Contractor warrants that it is duly qualified and shall perform its obligations under this Master Agreement in accordance with the commercially reasonable standards of care, skill, and diligence in Contractor's industry, trade, or profession, and in accordance with the specifications set forth in this Master Agreement, to the satisfaction of the Lead State.

c. Contractor warrants that it possesses the legal authority to enter into this Master Agreement and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Master Agreement, or any part thereof, and to bind Contractor to its terms.

3. **Awarded Band(s)**

The solicitation included three product Bands: Band 1, Personal Computing Devices – Windows Operating Systems: Desktops, Laptops, Tablets; and Band 2, Personal Computing Devices – Non-Windows Operating Systems: Desktops, Laptops, Tablets; and Band 3, Servers and Storage. The Contractor is awarded the following Band(s):

Band 1, Personal Computer Devices – Windows Operating Systems
Band 2, Personal Computer Devices - Non-Windows Operating Systems
Band 3, Servers and Storage

4. **Configuration Dollar Limits**

The following configuration limits apply to the Master Agreement. Participating Entities may define their configuration limits in their Participating Addendum. The Participating Entity's Chief Procurement Official may increase or decrease the configuration limits, as defined in their Participating Addendum. The Participating Entity will determine with the Contractor how to approve these modifications to the Product and Service Schedule.

The dollar limits identified below are based on a SINGLE computer/system configuration. This is NOT a restriction on the purchase of multiple configurations (e.g., an entity could purchase 10 laptops at $15,000 each, for a total purchase price of $150,000).

ITEM	CONFIGURATION
Band One	$15,000
Band Two	$15,000
Band Three	$1,000,000
Peripherals	$10,000
Services	Addressed in the Participating Addendum

5. **Restrictions**

The following restrictions apply to the Master Agreement. A Participating Entity may set further restrictions of products in their Participating Addendum. The Participating Entity will determine with the Contractor how to approve these modifications to the Entity's Product and Service Schedule.

a. Software

1. Software is restricted to operating systems and commercial off-the-shelf (COTS) software and is subject to equipment configuration limits.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

2. Any software purchased must be related to the procurement of equipment.

3. Software must be pre-loaded or provided as an electronic link with the initial purchase of equipment, except for the exceptions allowed under Paragraph 5.a.4.

4. Software such as middleware which is not always installed on the equipment, but is related to storage and server equipment (Band 3) purchased, is allowed and may be procured after the initial purchase of equipment.

b. General Services

1. Services must be related to the procurement of equipment.

2. Service limits will be addressed by each State.

3. Wireless phone and internet service is not allowed.

4. Managed Print Services are not allowed.

c. Cloud Services

1. Cloud Services are restricted to Services that function as operating systems and software needed to support or configure hardware purchased under the scope of the contract and is subject to equipment configuration limits.

2. Any Cloud Service purchased must be related to the procurement of equipment.

d. Third-Party Products

1. Third-Party Products can be offered only in the Bands they have been awarded. All third-party products must meet the definition(s) of the Band(s) in which they are being offered.

2. Products manufactured by another Contractor holding a Minnesota NASPO ValuePoint Master Agreement for Computer Equipment cannot be offered unless approved by the Lead State.

e. Additional Product/Services

1. Hardware and software required to solely support wide area network (WAN) operation and management are not allowed.

2. Lease/Rentals of equipment may be allowed and will be addressed by each State.

3. Cellular Phone Equipment is not allowed.

4. EPEAT Bronze requirement may be waived, on a State case-by-case basis, if approved by the State's Chief Procurement Officer. EPEAT Bronze requirement does not currently apply to storage.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

6. **Authorized Representative**

a. Master Agreement Administrator. The Master Agreement Administrator designated by NASPO ValuePoint and the State of Minnesota, Department of Administration is Elizabeth Randa, Acquisition Management Specialist.

Elizabeth Randa, Acquisition Management Specialist
Department of Administration
Office of State Procurement
112 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155
E-mail: elizabeth.randa@state.mn.us
Phone: 651.201.3122

b. Contractor's Authorized Representative. The Contractor's Authorized Representative is Ashley Salinas, SLED Contract Program Manager.

Ashley Salinas, SLED Contract Program Manager
Dell Inc.
One Dell Way
Round Rock, TX 78682
A.Salinas@dell.com
Phone: 512.542.1237

If the Contractor's Authorized Representative changes at any time during this Contract, the Contractor must immediately notify the Lead State.

7. **Notices**

If one party is required to give notice to the other under the Master Agreement, such notice shall be in writing and shall be effective upon receipt. Delivery may be by certified United States mail or by hand, in which case a signed receipt shall be obtained. An email shall constitute sufficient notice, provided the receipt of the transmission is confirmed by the receiving party. Either party must notify the other of a change in address for notification purposes. All notices to the Lead State shall be addressed to the Master Agreement Administrator.

8. **Exhibits**

The following Exhibits are attached and incorporated into this Contract. In the event of a conflict between the terms of this Contract and its Exhibits, or between Exhibits, the order of precedence is first the Contract, and then in the following order:

Exhibit A: NASPO ValuePoint Terms and Conditions
Exhibit B: Minnesota Terms and Conditions
Exhibit C: Requirement
Exhibit D: Price Schedule
Exhibit E: Contractor Terms and Conditions

9. **Survival of Terms:**

The following clauses survive the expiration or cancellation of this Master Agreement: Indemnification; State Audits; Government Data Practices and Intellectual Property; Publicity and Endorsement; Governing Law, Jurisdiction, and Venue; and Data Disclosure. Any other Contract term that states it shall survive, shall survive.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

10. **Entire Agreement**

This Contract and any written addenda thereto constitute the entire agreement of the parties to the Master Agreement.

1. Contractor

The Contractor certifies that the appropriate person(s) have executed the Contract on behalf of the Contractor as required by applicable articles, bylaws, resolutions, or ordinances.

Print name: Katherine Castillo

Signature: DocuSigned by: Katherine Castillo 8DEF23302D0B4B8...

Title: ParaLegal Advisor Date: 7/14/2023

2. State Agency

With delegated authority

Print name: Elizabeth M. Randa

Signature: DocuSigned by: Elizabeth M. Randa 742DE739C8ED492...

Title: Acquisition Management Specialist Date: 7/14/2023

3. Commissioner of Administration

As delegated to The Office of State Procurement

Print name: Andy Doran

Signature: DocuSigned by: Andy Doran 68D02A26D7604BA...

Title: IT Acquisitions Supervisor Date: 7/14/2023

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit A: NASPO ValuePoint Master Agreement Terms and Conditions

1. **Conflict of Terms/Order of Precedence.**

a. Any order placed under this Master Agreement shall consist of the following documents:

1. A Participating Entity's Participating Addendum ("PA");

2. Minnesota NASPO ValuePoint Master Agreement, as negotiated, including all exhibits;

3. A Purchase Order issued against a PA (terms and conditions set forth in a Purchase Order will not be deemed to modify, diminish, or otherwise derogate the terms and conditions set forth in a Participating Addendum or Minnesota NASPO ValuePoint Master Agreement).

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

c. Contractor terms and conditions may be incorporated if expressly accepted by the Lead State and attached to the Master Agreement as an Exhibit or Attachment, or by written reference (including reference to information contained in a URL or referenced policy). A written reference, including by URL or policy, is incorporated into the Master Agreement only if the Master Agreement expressly identifies that reference. URL's must be explicitly referenced to be incorporated into the Master Agreement. URL's contained within the URL's that are explicitly referenced are not incorporated into the Master Agreement. Any Contractor term or condition incorporated by URL or written reference applies to this Master Agreement only to the extent such term or condition is not prohibited by applicable law. Any change to information contained in a URL or referenced policy will not affect any financial obligation, place any additional material obligation on an ordering entity, or materially diminish an ordering entity's ability to use the product or service.

d. A written Master Agreement (which may include the contents of the RFP and selected portions of Contractor's response incorporated therein by reference) will constitute the entire agreement of the parties to the Master Agreement. No other terms and conditions shall apply, including terms and conditions listed in the Contractor's response to the RFP, or terms listed or referenced on the Contractor's website not otherwise incorporated into the Master Agreement, in the Contractor quotation/sales order, or in similar documents subsequently provided by the Contractor.

e. Additional Agreement with NASPO. Upon request by NASPO ValuePoint, awarded Contractor shall enter into a direct contractual relationship with NASPO ValuePoint related to Contractor's obligations to NASPO ValuePoint under the terms of the Master Agreement, the terms of which shall be the same or similar (and not less favorable) than the terms set forth in the Master Agreement.

2. **Definitions.**

a. **Acceptance** is defined by the applicable commercial code, except Acceptance shall not occur before the completion of delivery in accordance with the Order, installation if required, and a reasonable time for inspection of the Product.

b. **Accessory** means a product that enhances the user experience but does not extend the functionality of the computer (e.g. mouse pad or monitor stand). For the purposes of this Contract, accessories are considered peripherals.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

c. **_____ as a Service (_aaS)** refers to any good provided in a subscription-based model that is defined in the industry as "_____ as a Service". Examples are "Software as a Service", "Infrastructure as a Service", and "Storage as a Service", and shall follow the NIST definitions of those services. ____ as a Service are permitted only when they meet the restrictions found in Paragraph 5.c, above.

d. **Band** means a category of products. There are three product bands which may be awarded through this Contract. Each product band includes related peripherals and services.

e. **Components** are the parts that make up a computer configuration.

f. **Contractor** means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

g. **Configuration** means the combination of hardware and software components that make up the total functioning system.

h. **Customer** (see Purchasing Entity).

i. **Desktop** means a personal computer intended for regular use at a single location. A desktop computer typically comes in several units connected together during installation: (1) the processor, 2) display monitor, and 3) input devices usually a keyboard and a mouse. Desktops, including desktop virtualization endpoints such as zero and thin clients, are included in Bands 1 and 2 of this Contract.

j. **Embedded Software** means one or more software applications which permanently reside on a computing device.

k. **Energy Star®** is a voluntary energy efficiency program sponsored by the U.S. Environmental Protection Agency. The Energy Star program makes it easy to identify energy efficient computers by labeling products that deliver the same or better performance as comparable models while using less energy and saving money. For additional information on the Energy Star program, including product specifications and a list of qualifying products, visit the Energy Star website at http://www.energystar.gov.

l. **EPEAT** is a type-1 ecolabel for identifying and purchasing sustainable IT products. EPEAT-registered products must meet sustainability criteria detailed in voluntary consensus-based standards that are free and publicly available on the Green Electronics Council's website at www.greenelectronicscouncil.org. Products are classified as Bronze, Silver, or Gold based on meeting criteria that address the life cycle of the products. Product life cycle includes material extraction, hazardous substance reduction, end-of-life management, packaging, and corporate sustainability. Only products listed as Active in the online EPEAT Registry are considered to meet the EPEAT criteria.

m. **FOB Destination** means that shipping charges are included in the price of the item and the shipped item becomes the legal property and responsibility of the receiver when it reaches its destination unless there is acceptance testing required.

n. **FOB Inside Delivery** means that shipping charges are included in the price of the item, and that the shipped item becomes the legal property and responsibility of the receiver when it reaches the inside delivery point, which is beyond the front door or loading dock. FOB Inside Delivery is a special shipping arrangement that may include additional fees payable by the Purchasing Entity. FOB Inside Delivery must be annotated on the Purchasing Entity ordering document.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

o. **Intellectual Property** means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

p. **Laptop** means a personal computer for mobile use. A laptop includes a display, keyboard, point device such as a touchpad, and speakers in a single unit. A laptop can be used away from an outlet using a rechargeable battery. Laptops include notebooks, ultrabooks, netbooks, Zero and thin client devices, and computers with mobile operating systems. Laptops are included in Bands 1 and 2 of this Contract.

q. **Lead State** means the State centrally administering any resulting Master Agreement(s).

r. **Mandatory Requirement** is a requirement that the failure to meet results in the rejection of the responder's proposal unless all responders are unable to meet the mandatory requirement. The terms "must" and "shall" identify a mandatory requirement. Any objection to a mandatory requirement should be identified by responders in the Question and Answer period.

s. **Manufacturer** means a company that, as one of its primary business functions, designs, assembles, owns the trademark/patent for, and markets branded computer equipment.

t. **Master Agreement** means the underlying agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor.

u. **Middleware** means the software "glue" that helps programs and databases (which may be on different computers) work together. The most basic function of middleware is to enable communication between different pieces of software.

v. **NASPO ValuePoint** is a division of the National Association of State Procurement Officials ("NASPO"), a 501(c)(3) limited liability company. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports as well as other contract administration functions as assigned by the Lead State.

w. **Option** means an item of equipment or a feature that may be chosen as an addition to or replacement for standard equipment and features.

x. **Order or Purchase Order** means any purchase order, sales order, contract or other method used by a Purchasing Entity to order the Products.

y. **Participating Addendum** means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

z. **Participating Entity** means a state (as well as the District of Columbia and U.S territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states properly authorized to enter into a Participating Addendum, that has executed a Participating Addendum.

aa. **Participating State** means a state that has executed a Participating Addendum.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

bb. **Partner** means a company, authorized by the Contractor and approved by the Participating Entity, to provide marketing, support, or other authorized contract services on behalf of the Contractor in accordance with the terms and conditions of the Contractor's Master Agreement. A Partner may include, but is not limited to, an agent, subcontractor, fulfillment partner, channel partner, business partner, servicing subcontractor, etc.

cc. **Peripherals** means any hardware product that can be attached to, added within, or networked with personal computers, servers, or storage. Peripherals extend the functionality of a computer without modifying the core components of the system.

dd. **Per Transaction Multiple Unit Discount** means a contractual volume discount based on dollars in a single purchase order or combination of purchase orders submitted at one time by a Participating Entity or multiple entities conducting a cooperative purchase.

ee. **Premium Savings Package(s) (PSP)** are deeply discounted standard configurations available to Purchasing Entities using the Master Agreement. NASPO ValuePoint reserves the right to expand and modify the PSP throughout the life of the contract. For more information see: https://www.naspovaluepoint.org/portfolio/57/.

ff. **Product** means any equipment, software (including embedded software), documentation, service, or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Products, supplies and services, and products and services are used interchangeably in these terms and conditions.

gg. **Purchasing Entity** means a state (including the District of Columbia and U.S. territories), city, county, district, other political subdivision of a state, other public entities domestic or foreign, and nonprofit organizations under the laws of some states if authorized by a Participating Addendum, that issues a Purchase Order under the terms of the Master Agreement, or any Participating Addendum thereto, and becomes financially committed to the purchase.

hh. **Ruggedized** means equipment specifically designed to operate reliably in harsh usage environments and conditions, such as strong vibrations, extreme temperatures, and wet or dusty conditions. Ruggedized equipment may be proposed under the band that most closely fits the equipment being proposed.

ii. **Server** means computer hardware dedicated to run one or more services or applications (as a host) to serve the needs of the users of other computers on a network. Servers may be either physical or virtual. Servers, including server appliances, are included in Band 3 of this Contract. Server appliances have their hardware and software preconfigured by the manufacturer, and include embedded networking components such as those found in blade chassis systems.

jj. **Services** are broadly classified as installation or de-installation, maintenance, support, training, migration, and optimization of products offered or supplied under the Master Agreement. These classifications of services may include, but are not limited to: warranty services, maintenance, installation, de-installation, factory integration (software or hardware components), asset management, recycling or disposal, training and certification, pre-implementation design, disaster recovery planning and support, service desk or helpdesk, imaging, and any other directly related technical support service required for the effective operation of a product offered or supplied. Contractors may offer limited professional services related ONLY to the equipment and configuration of the equipment purchased through the resulting contracts.

EACH PARTICIPATING ENTITY WILL DETERMINE RESTRICTIONS AND NEGOTIATE TERMS FOR SERVICES THROUGH THEIR PARTICIPATING ADDENDUM.

kk. **Software** means, for the purposes of this Contract, commercial operating off the shelf machine-readable object code instructions including microcode, firmware, and operating system software that meet the restrictions specified

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

in Paragraph 5.a. “Software” applies to all parts of software and documentation, including new releases, updates, and modifications of software.

ll. **Storage** means hardware or a virtual appliance with the ability to store large amounts of data. Storage, including SAN switching necessary for the proper functioning of storage equipment, is included in Band 3 of this Contract

mm. **Storage Area Network (SAN)** is a high-speed special-purpose network (or subnetwork) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

nn. **Tablet** means a mobile computer that provides a touchscreen that acts as the primary means of control. Tablets, including notebooks, ultrabooks, and netbooks with touchscreen capabilities, are included in Bands 1 and 2 of this Contract.

oo. **Takeback Program** means the Contractor’s process for accepting the return of equipment or other products at the end of the product’s life.

pp. **Thin Client** is a lightweight computer that has been optimized for establishing a remote connection with a server-based computing environment.

qq. **Third Party Product** is a good sold by the Contractor that is manufactured by another company. Third Party Products are intended to enhance or supplement a Contractor’s own product line, and are not intended to represent more than a third of any Contractor’s total sales under this Master Agreement.

rr. **Upgrade** means the replacement of existing software, hardware, or hardware component with a newer version.

ss. **Warranty** means the Manufacturer’s general warranty tied to the product at the time of purchase.

tt. **Wide Area Network (WAN)** is a data network that serves users across a broad geographic area and often uses transmission devices provided by common carriers.

3. **Term of the Master Agreement.**

a. The initial term of this Master Agreement is for 2 years. This Master Agreement may be extended beyond the original contract period for 36 additional months at the Lead State’s discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance.

b. The Master Agreement may be extended for a reasonable period of time if in the judgment of the Lead State a follow-on, competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection shall not be deemed to limit the authority of a Lead State under its state law otherwise to negotiate contract extensions.

4. **Amendments.**

The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without a written amendment to the Master Agreement executed by the Contractor and Lead State as required by law. Master Agreement amendments will be negotiated by the Lead State with the Contractor whenever necessary to address changes in the terms and conditions, costs, timetable, or increased or decreased scope of work.

5. **Participants and Scope.**

a. Canadian Participation. Subject to the approval of Contractor, any Canadian provincial government or provincially funded entity in Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador,

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Nova Scotia, Ontario, Prince Edward Island, Quebec, or Saskatchewan, and territorial government or territorial government funded entity in the Northwest Territories, Nunavut, or Yukon, including municipalities, universities, community colleges, school boards, health authorities, housing authorities, agencies, boards, commissions, and crown corporations, may be eligible to use Contractor's Master Agreement. Canadian Participation. Subject to the approval of the Contractor, any Canadian provincial government or provincially funded entity in Ontario, Quebec, Nova Scotia, New Brunswick, Manitoba, British Columbia, Prince Edward Island, Saskatchewan, Alberta, Northwest Territories, Nunavut, Yukon, and Newfoundland and Labrador, including municipalities, universities, community colleges, school boards, health authorities, housing authorities, agencies, boards, commissions, and crown corporations, may be eligible to use Contractor's Master Agreement.

b. Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

c. Use of specific NASPO ValuePoint Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating Entities who are states are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating Entities who are states incur no financial obligations on behalf of other Purchasing Entities. Contractor shall email a fully executed PDF copy of each Participating Addendum to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

e. NASPO and NASPO ValuePoint are not parties to the Master Agreement.

f. Participating Addenda shall not be construed to amend the following provisions in this Master Agreement between the Lead State and Contractor that prescribe NASPO ValuePoint requirements: Term of the Master Agreement; Amendments; Participants and Scope; Administrative Fee; NASPO ValuePoint Summary and Detailed Usage Reports; NASPO ValuePoint Cooperative Program Marketing and Performance Review; Right to Publish; Price and Rate Guarantee Period; and Individual Customers. Any such language shall be void and of no effect.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the consent to participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

h. Resale. "Resale" means any payment in exchange for transfer of tangible goods, software, or assignment of the right to services. Subject to any specific conditions included in the Master Agreement, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products (the definition of which includes services that are deliverables). Absent any such condition or explicit permission, this limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

6. **Individual Customers.**

Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

7. **Independent Contractor.**

The Contractor is an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as an agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

8. **Contracting Personnel.**

Contractor must provide adequate contracting personnel to assist states with the completing and processing Participating Addenda. It is preferred that each Contractor be able to provide each Participating Entity with a primary contact person for that Participating Entity.

9. **Changes in Contractor Representation.**

The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel managing the Master Agreement in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. Such approval shall not be unreasonably withheld. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

10. **Contractor Verification.**

The Contractor is responsible for delivering products or performing services under the terms and conditions set forth in the Master Agreement. The Contractor must ensure partners utilized in the performance of this contract adhere to all the terms and conditions. The term Partner will be utilized in naming the relationship a Contractor has with another company to market and sell under the contract. Participating Entities will have final determination/approval if a Partner may be approved for that state in the role identified by the Contractor.

11. **Contractor Performance Meeting.**

An annual performance meeting may be held each year with the NASPO ValuePoint Sourcing Team. Historically performance meetings have been held in Minnesota, but the Lead State may hold the meetings in person or virtually at the Lead State's discretion.

All contractors that are invited to participate must send their Primary Account Representative, unless an exception is granted in writing by the Lead State. It is possible that not all contractors will be invited to participate in a performance meeting.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

12. **Laws and Regulations.**
Any and all Products offered and furnished shall comply fully with all applicable Federal, State, and local laws and regulations, including Minn. Stat. § 181.59 prohibiting discrimination and business registration requirements of the Office of the Minnesota Secretary of State. To the extent any purchase is subject to Federal Acquisition Regulations, as may be required by the terms of a federal grant, a Participating Entity and Contractor may include in their Participating Addendum terms that reflect such a requirement.

13. **Price and Rate Guarantee Period.**
All minimum discounts and rates must be guaranteed for the initial term of the Master Agreement. Following the initial Master Agreement period, any request for minimum discount or rate adjustment must be for a guarantee period as offered by the Contractor, and must be made at least 30 days prior to the effective date. Requests for minimum discount or rate adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the Master Agreement shall not be effective unless approved by the Lead State. No retroactive adjustments to minimum discounts or rates will be allowed.

14. **Premium Savings Package Program.**
The Lead State reserves the right to create a Premium Savings Package Program (PSP) as outlined in the Definitions, Paragraph 2.ee of Exhibit A. Participation by Contractor is voluntary. The details and commitments of the PSP will be detailed as a part of any request for Contractor to participate.

15. **Services.**
Participating Entities must explicitly allow services in their Participating Addenda for the approved services to be allowed under that Participating Addendum. The Participating Addendum by each Participating Entity will address service agreement terms and related travel.

16. **Ordering.**

a. Master Agreement and purchase order numbers shall be clearly shown on all acknowledgments, packing slips, invoices, and on all correspondence.

b. Purchasing Entities may define entity or project-specific requirements and informally compete the requirement among companies having a Master Agreement on an “as needed” basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity’s rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities’ rules, policies, and procedures regarding the ordering of supplies or services contemplated by this Master Agreement.

d. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document under the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

1. The service description or supplies being delivered;

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

2. The place and requested time of delivery;

3. A billing address;

4. The name, phone number, and address of the Purchasing Entity representative;

5. The price per hour or other pricing elements consistent with this Master Agreement and the contractor's proposal;

6. A ceiling amount of the order for services being ordered;

7. The Master Agreement identifier; and

8. Statement of Work, when applicable.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation or termination of this Master Agreement, or otherwise inconsistent with its terms. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

17. **Trade-In.**

Any trade-in programs offered during the life of the Master Agreement must be approved by the Lead State. Participating Entities must explicitly allow trade-in programs in their Participating Addenda for the approved programs to be allowed under that Participating Addendum. Trade-in value shall not decrease the discounts offered through the Master Agreement.

18. **Shipping and Delivery.**

a. The prices are the delivered price to any Purchasing Entity for standard 3-5 day shipping. If an order is requested with expedited shipping, the Contractor must provide a firm "not to exceed" price for the expedited shipping on the quote. All deliveries shall be FOB Destination, freight pre-paid, with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage shall remain the Contractor's until final inspection and acceptance when responsibility shall pass to the Purchasing Entity except as to latent defects, fraud and Contractor's warranty obligations. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered shall be shipped without charge.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

b. Specific delivery instructions, including FOB Inside Delivery, will be noted on the order form or Purchase Order. Any damage to the building interior, scratched walls, damage to the freight elevator, etc., will be the responsibility of the Contractor. If damage does occur, it is the responsibility of the Contractor to promptly notify the Purchasing Entity placing the Order.

c. All products must be delivered in the manufacturer's standard package. Costs shall include all packing and crating charges. Cases shall be of durable construction, good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipment shall be marked with the Purchasing Entity's Purchase Order number and other information sufficient for the Purchasing Entity to properly identify the shipment as outlined in the Participating Addendum of the Purchasing Entity.

19. **Inspection and Acceptance.**

a. Where the Master Agreement, a Participating Addendum, or an Order does not otherwise specify a process for inspection and Acceptance, this section governs. This section is not intended to limit rights and remedies under the applicable commercial code.

b. Acceptance. Purchasing Entity shall determine whether all Products and Services delivered meet the Contractor's published specifications. No payment shall be made for any Products or Services until the Purchasing Entity has accepted the Products or Services. The Purchasing Entity will make every effort to notify the Contractor within thirty (30) calendar days following delivery of non-acceptance of a Product or completion of Service. In the event that the Contractor has not been notified within 30 calendar days from delivery of Product or completion of Service, the Product and Services will be deemed accepted on the 31st day after delivery of Product or completion of Services. Failure to reject upon receipt, however, does not relieve the Contractor of liability for latent or hidden material defects. Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked. The warranty period shall begin upon Acceptance. If the parties agree to acceptance testing, the terms of subsection (c), below, apply.

c. Acceptance Testing. The Purchasing Entity and the Contractor shall determine if Acceptance Testing is applicable and required for the purchase. "Acceptance Testing" means the process for ascertaining that the Product meets the standard of performance prior to Acceptance by the Purchasing Entity.

1. The Acceptance Testing period shall be thirty (30) calendar days starting from the day after the Product is delivered or, if installed, the day after the Product is installed and Contractor certifies that the Product is ready for Acceptance Testing. If the Product does not meet the standard of performance during the initial period of Acceptance Testing, Purchasing Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the standard of performance is met. Upon rejection, the Contractor will have fifteen (15) calendar days to cure the standard of performance issue(s). If after the cure period, the Product still has not met the standard of performance, the Purchasing Entity may, at its option: (a) declare Contractor to be in breach and terminate the Order; (b) demand replacement Product from Contractor at no additional cost to Purchasing Entity; or, (c) continue the cure period for an additional time period agreed upon by the Purchasing Entity and the Contractor.

2. No Product shall be deemed Accepted and no charges shall be paid until the standard of performance is met. Products that do not meet specifications may be rejected. Failure to reject upon receipt, however, does not relieve the Contractor of liability for material (nonconformity that substantially impairs value) latent or hidden defects subsequently revealed when goods are put to use. Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked. The warranty period shall begin upon Acceptance.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

d. If any services do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and reduce the contract price to reflect the reduced value of services performed.

20. **Title of Product.**

a. Definitions. For purposes of this section, the following terms are defined as follows:

1. “Deliverables” means any reports, analyses, scripts, code, or other work results that Contractor delivers to Purchasing Entity within the framework of fulfilling Contractor’s obligations to Purchasing Entity.

2. "Equipment” means Contractor-branded hardware products.

3. “Proprietary Rights” means all patents, copyrights, trademarks, trade secrets, and other intellectual property rights of a party.

b. Upon Acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Equipment free and clear of all liens, encumbrances, or other security interests. Purchasing Entity’s rights to use the software delivered by Contractor are governed by the terms of the applicable end-user license agreement. Unless different terms have been agreed between the parties, the terms posted on www.dell.com/eula (the “EULA”) shall apply. Contractor’s EULA must be made available to Purchasing Entities for review prior to negotiating a Participating Addendum or the issuance of an Order and shall meet or exceed the terms set forth in this Master Agreement. Unless expressly otherwise agreed, microcode, firmware or operating system software required to enable the Equipment with which it is shipped to perform its basic or enhanced functions, is licensed for use solely on such Equipment.

c. Contractor grants Purchasing Entity a non-exclusive, non-transferable, irrevocable license to use (without the right to sublicense) the Deliverables provided by Contractor for Purchasing Entity’s internal business and governmental purposes, only and solely in accordance with the applicable service specification and subject to this Master Agreement. The grant of this license is subject to Purchasing Entity’s compliance with the terms of this Master Agreement and Purchasing Entity’s payment of applicable amounts due. Such license shall be perpetual unless granted pursuant to the purchase of a subscription, in which case the license shall be for the term of the subscription. Purchasing Entity may authorize its service providers to use the Deliverables, but solely on Purchasing Entity’s behalf, solely for Purchasing Entity’s internal business or governmental purposes, and Purchasing Entity shall be responsible for service provider’s compliance with these restrictions. This section shall not affect a Purchasing Entity’s right to transfer ownership of a product, and transfer, if permitted by Contractor or its licensors, licenses associated with such product, to another individual or entity as part of the Purchasing Entity’s surplus program or sale of used products to employees or former employees.

d. Contractor reserves for itself all Proprietary Rights that it has not expressly granted to Purchasing Entity herein. The license granted in this clause 20(c) does not apply to: (i) Equipment; (ii) Contractor-branded generally available software; or (ii) items licensed or otherwise provided under a separate agreement. Contractor is not limited in developing, using, or marketing services or products that are similar to the Deliverables or Professional Services provided hereunder, any service, specification, or, subject to Contractor’s confidentiality obligations to Purchasing Entity, in using the Deliverables or performing similar Professional Services for any other projects. Notwithstanding the previous, Contractor’s use of Deliverables created specifically for and paid for by a Purchasing Entity is subject to Purchasing Entity approval.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

e. Any and all licensing, maintenance, cloud services, or order specific agreements referenced within the terms and conditions of this Master Agreement are agreed to only to the extent that the terms do not conflict with the terms of the Participating Addendum or the terms of the Master Agreement as incorporated into the Participating Addendum, and to the extent the terms are not in conflict with the Participating Entity's applicable laws. In the event of a conflict in the terms and conditions, the conflict shall be resolved as detailed in the Order of Precedence defined herein. Notwithstanding the foregoing, licensing, maintenance, cloud services agreements, or order specific agreements may be further negotiated by the Contractor or, if applicable, the Licensor, and the potential Purchasing Entity, provided the contractual documents are duly executed in writing.

f. If (i) Contractor is or becomes aware of any infringement claim made against a third-party branded product offered by Contractor through this Master Agreement, (ii) the third-party branded product is determined to infringe upon the intellectual property rights of another third party, and (iii) such infringement is not remedied by the third party so that the product is no longer infringing, Contractor shall immediately cease offering the product under this Master Agreement and notify the Lead State, NASPO, Participating Entities, and purchasers of the product.

21. **Warranty.**

The Contractor must ensure warranty service and maintenance for all equipment, including third party products provided. The Contractor must facilitate the Manufacturer or Publisher warranty and maintenance of third party products furnished through the Master Agreement. The Contractor shall provide the warranty service and maintenance for equipment and all peripherals on the Master Agreement.

22. **System Failure or Damage.**

In the event of system failure or damage caused by the Contractor or its Product, the Contractor shall use reasonable efforts to restore or assist in restoring the system to operational capacity. The Contractor shall be responsible under this provision to the extent a 'system' is defined at the time of the Order; otherwise the rights of the Purchasing Entity shall be governed by the Warranty.

23. **Payment.**

Payment after Acceptance is normally made within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum, Order, or otherwise prescribed by applicable law.

Payments will be remitted by mail or electronically. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

Prices are exclusive of taxes, duties, and fees, unless otherwise quoted. If a withholding tax is required by law, the tax will be added and identified on the applicable invoice. All applicable taxes, duties, and fees must be identified on the quote.

24. **Leasing or Alternative Financing Methods.**

Lease purchase and term leases are allowable only for Purchasing Entities whose rules and regulations permit leasing of software. Individual Purchasing Entities may enter into a lease agreement for the products covered in this Master Agreement, if they have the legal authority to enter into these types of agreements without going through a competitive process and if the applicable PAs permit leasing. No lease agreements will be reviewed or evaluated as part of the RFP evaluation process.

25. **Contract Provisions for Orders Utilizing Federal Funds.**

Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this Master Agreement.

26. **Self Audit.**
The Contractor must conduct at a minimum a quarterly self-audit, unless approved by the Lead State. The audit will sample a minimum of one tenth of one percent (.001) of orders with a maximum of 100 audits per quarter conducted. For example: Up to 1,000 sales = 1 audit; 10,000 sales = 10 audits; Up to 100,000 sales = 100 audits. This will be a random sample of orders and invoices and must include documentation of pricing. Summary findings must be reported to Lead State with actions to correct documented findings.

27. **Assignment/Subcontracts.**

a. Contractor shall not assign, sell or otherwise transfer all or any part of this Master Agreement without prior written consent from the Lead State, such consent not to be unreasonably withheld.

b. The Lead State, or Participating Entity, shall not assign, delegate or otherwise transfer all or any part of this Master Agreement without prior written consent from Contractor, except for assignment or delegation to a Participating Entity State agency or eligible Purchasing Entity. The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to NASPO ValuePoint and other third parties.

28. **Insurance.**

a. Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers legally authorized to conduct business in the Lead State and in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below:

1. Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$2 million general aggregate;

2. Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

c. Contractor shall pay premiums on all insurance policies. Contractor will use reasonable efforts to give thirty (30) days prior written notice to State prior to cancellation or non-renewal of any of the policies providing such coverage; provided, however that Contractor shall not be obligated to provide such notice if, concurrently with such cancellation or non-renewal, Contractor obtains coverage from different insurer(s) meeting the requirements described herein.

d. Prior to commencement of performance, Contractor shall provide to the Participating Entity a certificate of insurance showing the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating Entity as an additional insured, (2) provides that written notice of cancellation shall be delivered in accordance with the policy provisions, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating Entity as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, other state Participating Entities' rights

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

and Contractor's obligations are the same as those specified in the first sentence of this subsection except the endorsement is provided to the applicable state.

e. During the term of this Master Agreement, Contractor shall upon request provide to the Lead State and Participating Entities evidence of coverage that meets the requirements of this Section and the applicable Participating Addendum. Failure to provide evidence of coverage, within thirty (30) calendar days of receipt of request may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

29. **Administrative Fees.**

a. The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on all sales of products and services under the Master Agreement (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not negotiable.

b. The NASPO ValuePoint Administrative Fee in this section shall be based on the gross amount of all sales (less any charges for taxes or shipping) at the adjusted prices (if any) in Participating Addenda.

c. Additionally, some states may require an additional fee be paid directly to the state only on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Purchasing Entity may allow the Contractor to adjust the Master Agreement pricing to account for these additional fees for purchases made by Purchasing Entities within the jurisdiction of the Participating Entity. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee.

30. **NASPO ValuePoint Reports**

a. Sales Data Reporting. In accordance with this section, Contractor shall report to NASPO ValuePoint all Orders under this Master Agreement for which Contractor has invoiced the ordering entity or individual, including Orders invoiced to Participating Entity or Purchasing Entity employees for personal use if such use is permitted by this Master Agreement and the applicable Participating Addendum ("Sales Data"). Timely and complete reporting of Sales Data is a material requirement of this Master Agreement. Reporting requirements, including those related to the format, contents, frequency, or delivery of reports, may be updated by NASPO ValuePoint with reasonable notice to Contractor and without amendment to this Master Agreement. NASPO ValuePoint shall have exclusive ownership of any media on which reports are submitted and shall have a perpetual, irrevocable, non-exclusive, royalty free, and transferable right to display, modify, copy, and otherwise use reports, data, and information provided under this section.

b. Summary Sales Data. "Summary Sales Data" is Sales Data reported as cumulative totals by state. Contractor shall, using the reporting tool or template provided by NASPO ValuePoint, report Summary Sales Data to NASPO ValuePoint for each calendar quarter no later than thirty (30) days following the end of the quarter. If Contractor has no reportable Sales Data for the quarter, Contractor shall submit a zero-sales report.

c. Detailed Sales Data. "Detailed Sales Data" is Sales Data that includes for each Order all information required by the Solicitation or by NASPO ValuePoint, including customer information, Order information, and line-item details.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Contractor shall, using the reporting tool or template provided by NASPO ValuePoint, report Detailed Sales Data to NASPO ValuePoint for each calendar quarter no later than thirty (30) days following the end of the quarter. Detailed Sales Data shall be reported in the format provided in the Solicitation or provided by NASPO ValuePoint. The total sales volume of reported Detailed Sales Data shall be consistent with the total sales volume of reported Summary Sales Data.

d. Sales Data Crosswalks. Reserved.

e. Executive Summary. Contractor shall, upon request by NASPO ValuePoint, provide NASPO ValuePoint with an executive summary that includes but is not limited to a list of states with an active Participating Addendum, states with which Contractor is in negotiations, and any Participating Addendum roll-out or implementation activities and issues. NASPO ValuePoint and Contractor will determine the format and content of the executive summary.

31. **NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review.**

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the Participating Entity. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the Participating Entity.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, cancel the Master Agreement pursuant to Paragraph 42 of Exhibit A, or not exercise an option to renew, when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if contractor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than two years after award of the Master Agreement. This subsection does not limit the discretionary right of either the Lead State or Contractor to cancel the Master Agreement pursuant to Paragraph 42 of Exhibit A or to terminate for default pursuant to Paragraph 44 of Exhibit A.

g. Contractor agrees to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in any Cooperative Purchasing Agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions. For the purposes of this paragraph, Cooperative Purchasing Agreement shall mean a cooperative

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

purchasing program facilitating public procurement solicitations and agreements using a lead agency model. This does not include contracts with any federal agency or any federal contract.

32. **Right to Publish.**

Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the public release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan. The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

33. **Records Administration and Audit.**

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's state statutes, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

34. **Indemnification**

a. General Indemnity. Contractor shall indemnify, defend (to the extent permitted by a state's Attorney General), and hold harmless an Indemnified Party from any claims or causes of action, including attorney's fees, to the extent arising from Contractor's intentional, willful, or negligent acts or omissions; actions that give rise to strict liability; and actions arising from breach of contract or warranty.

"Indemnified Party" means NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the Indemnified Party's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the Indemnified Party's failure to fulfill its obligation under this Contract.

b. Intellectual Property Indemnification.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

1. In the event of any such claim by any third party against the Indemnified Party that Products, Software, Services or Deliverables prepared, produced, or branded by Contractor and delivered pursuant to this Master Agreement infringe or misappropriate that third party's U.S. patent, copyright, trade secret, or other intellectual property rights ("Indemnified Claims"), the Indemnified Party shall promptly notify the Contractor. The Contractor, at its own expense, shall indemnify, defend to the extent permitted by the Indemnified Party's laws, and hold harmless the Indemnified Party against any loss, cost, expense, or liability (including legal fees) arising out of such a claim, whether or not such claim is successful against the Indemnified Party.

2. If Contractor receives prompt notice of such a claim that in the Contractor's opinion is likely to result in an adverse ruling, the Contractor shall at its option (1) obtain a right for the Indemnified Party to continue using such Products, Deliverables, or Software or allow Contractor to continue performing the Services; (2) modify such Products, Software, Services, or Deliverables to make them non-infringing without materially affecting their utility or functionality; (3) replace such Products, Software, Services, or Deliverables with a non-infringing equivalent; or (4) refund any pre-paid fees for the allegedly infringing Services that have not been performed or provide a reasonable depreciated or pro rata refund for the allegedly infringing Product, Deliverables, or Software.

3. Notwithstanding the foregoing, Contractor shall have no obligation under this Section for any claim resulting or arising from (1) modifications of the Products, Software, Services, or Deliverables that were not performed by, on behalf of, or at the direction of Contractor; (2) the combination, operation, or use of the Products, Software, Services, or Deliverables in connection with a third-party product, software or service (the combination of which causes the claimed infringement); or (3) Contractor's compliance with Indemnified Party's written specifications or directions, including the incorporation of any software or other materials or processes provided by or requested by Indemnified Party. Contractor's duty to indemnify and defend under this Section is contingent upon: (a) Contractor receiving prompt written notice of the third-party claim or action for which Contractor must indemnify Indemnified Party, (b) Contractor having the right to solely control the defense and resolution of such claim or action, unless the Indemnified Party's law requires approval for a third party to defend the Indemnified Party and such approval is not received, and (c) Indemnified Party's cooperation with Contractor in defending and resolving such claim or action. This Section states Indemnified Party's exclusive remedies for any third-party intellectual property claim or action and nothing in this Master Agreement or elsewhere will obligate Contractor to provide any greater indemnity to Indemnified Party.

35. **Limitations of Liability**

a. The Parties agree that neither Contractor nor the indemnified party shall be liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages except any claim related to bodily injury or death; an unauthorized release or breach of not public data as set forth more fully in Minn. Ch. 13; or a claim or demand based on patent, copyright, or other intellectual property infringement.

b. Contractor's liability is limited to 2 times the amount paid by Purchasing Entity to Contractor during the 12 months preceding the date of the dispute concerning any products and services, or $5,000,000, whichever is greater. This limit on liability does not apply to claims for bodily injury or death or for intellectual property infringement.

c. Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:

1. provided by the Contractor or the Contractor's subsidiaries or affiliates;

2. specified by the Contractor to work with the Product; or

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

3. reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

4. It would be reasonably expected to use the Product in combination with such product, system or method.

36. **License of Pre-Existing Intellectual Property.**
Intentionally deleted.

37. **Assignment of Antitrust Rights.**
Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

38. **Debarment.**
The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

39. **Governing Law and Venue.**

a. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State. The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to contract performance or administration if the Lead State is a party; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

40. **Confidentiality, Non-Disclosure, and Injunctive Relief.**

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's clients.

1. Any and all information of any form that is marked as confidential by one party (the "originating party") and is or would by its nature be deemed confidential obtained by the other party or its employees or agents (the "receiving party") in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of the originating party ("Confidential Information").

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

2. Any reports or other documents or items (including software) that result from the use of the Confidential Information by the receiving party shall be treated in the same manner as the Confidential Information.

3. Confidential Information does not include information that (1) is or becomes (other than by disclosure by the receiving party) publicly known; (2) is furnished by the originating party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than the originating party without the obligation of confidentiality, (5) is disclosed with the written consent of the originating party or; (6) is independently developed by employees, agents or subcontractors of the receiving party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. The receiving party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement.

1. Each party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information.

2. Without limiting the generality of the foregoing, the receiving party shall advise the originating party, and the applicable Participating Entity, and the Lead State if the originating party is a Purchasing Entity, and the Lead State if the originating party is a Participating Entity, immediately if the receiving party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and the receiving party shall at its expense cooperate with advise the originating party in seeking injunctive or other equitable relief in the name of either party against any such person.

3. Except as directed by the originating party, the receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at the originating party's request, the receiving party shall turn over to the originating party all documents, papers, and other matter in the receiving party's possession that embody Confidential Information.

4. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement, and Purchasing Entity may retain Confidential Information to the extent and for the duration required by applicable law.

c. Injunctive Relief. Each party acknowledges that the other party's breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to originating party that is inadequately compensable in damages. Accordingly, the originating party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

e. The rights granted Purchasing Entities and Contractor obligations under this section shall also extend to the cooperative's Confidential Information, defined to include Participating Addenda, as well as Orders or transaction data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line item

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to Paragraph 33 of Exhibit A. To the extent permitted by law, Contractor shall notify the Lead State of the identity of any entity seeking access to the Confidential Information described in this subsection.

41. **Public Information.**
This Master Agreement and all related documents are subject to disclosure pursuant to the Lead State's public information laws.

42. **Cancellation.**
Unless otherwise set forth in this Master Agreement, this Master Agreement may be canceled by either party upon 60 days written notice prior to the effective date of the cancellation. Further, any Participating Entity may cancel its participation upon 30 days written notice, unless otherwise stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision shall not affect the rights and obligations attending orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate as set forth in Paragraph 44 of Exhibit A.

43. **Force Majeure.**
Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, unusually severe weather, other acts of God, or war which are beyond that party's reasonable control. The Lead State may terminate this Master Agreement after determining such delay or default will reasonably prevent successful performance of the Master Agreement.

44. **Defaults and Remedies.**

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

1. Nonperformance of contractual requirements; or

2. A material breach of this Master Agreement; or

3. Any certification, representation or warranty by Contractor in response to the RFP or in this Master Agreement that proves to be untrue or materially misleading; or

4. Institution of proceedings under any bankruptcy, insolvency, court-ordered reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

5. Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, except for material breach, the Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement. The Lead State may immediately terminate this Master Agreement upon material breach of the Master Agreement by Contractor.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

1. Exercise any remedy provided by law; and
2. Terminate this Master Agreement and any related contracts or portions thereof; and
3. Impose liquidated damages as provided in this Master Agreement; and
4. Suspend Contractor from being able to respond to future bid solicitations; and
5. Suspend Contractor's performance; and
6. Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and shall have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless otherwise specified in a Purchase Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

45. **Waiver of Breach.**

Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

46. **Notices.**

If one party is required to give notice to the other under the Master Agreement, such notice shall be in writing and shall be effective upon receipt. Delivery may be by certified United States mail or by hand, in which case a signed receipt shall be obtained. A facsimile or electronic transmission shall constitute sufficient notice, provided the receipt of the transmission is confirmed by the receiving party. Either party must notify the other of a change in address for notification purposes. All notices to the Lead State shall be addressed as follows:

Elizabeth Randa, Acquisition Management Specialist
112 Administration Bldg.
50 Sherburne Avenue
St. Paul, MN 55155
elizabeth.randa@state.mn.us

47. **No Waiver of Sovereign Immunity.**

In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the state of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit B: Minnesota Terms and Conditions

1. **Change Requests.**

The Lead State reserves the right to request, during the term of the Master Agreement, changes to the products offered within the Band(s). Products introduced during the term of the Master Agreement shall go through a formal review process. The process for updating the products offered within a Band is outlined in Paragraph 2 of Exhibit B. The Contractor shall evaluate and recommend products for which agencies have an expressed need. The Lead State shall require the Contractor to provide a summary of its research of those products being recommended for inclusion in the Master Agreement as well as defining how adding the product will enhance the Master Agreement. The Lead State may request that products, other than those recommended, are added to the Master Agreement.

In the event that the Lead State desires to add new products and services that are not included in the original Master Agreement, the Lead State requires that independent manufacturers and resellers cooperate with the already established Contractor in order to meet the Lead State's requirements. Evidence of the need to add products or services should be demonstrated to the Lead State. The Master Agreement shall be modified via supplement or amendment. The Lead State will negotiate the inclusion of the products and services with the Contractor. No products or services will be added to the Master Agreement without the Lead State's prior approval.

2. **Product and Service Schedule (PSS).**

a. Creating the Product and Service Schedule (PSS). Contractor will use the attached sample PSS to create and maintain a complete listing of all products and services offered under the Master Agreement. The PSS must conform to the contracted minimum discounts. Contractor may create and maintain a separate PSS for a Participating Entity based on the requirements and restrictions of the Participating Entity.

Contractors are encouraged to provide remote learning bundles for K-12 Education. These bundles can be included in the response to the PSS.

b. Maintaining the PSS.

1. In General. Throughout the term of the Master Agreement, on a quarterly basis, Contractor may update the PSS to make model changes, add new products or services, or remove obsolete or discontinued products or services. Any updates to the PSS must conform to the Master Agreement requirements, including the scope of the Master Agreement and contracted minimum discounts.

2. Process. Contractor must provide notification to the Lead State of any changes to their PSS using the attached Action Request Form (ARF).

a) The Lead State does not need to approve Contractor's request to make model changes, add their own manufactured products, or remove discontinued or obsolete products or services, and Contractor does not need the Lead State's approval prior to posting an updated PSS.

b) The Lead State must approve Contractor's request to add new third party manufacturers to Contractor's PSS. If the proposed third-party manufacturer holds a NASPO Master Agreement for Computer Equipment, Contractor must obtain written authorization from that manufacturer. Contractor must have the Lead State's approval prior to posting the updated PSS.

c) Contractor must maintain a historic record of all past PSSs on their dedicated NASPO ValuePoint website.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

d) Pursuant to the audit provisions of the Master Agreement, upon the request of NASPO ValuePoint, the Lead State, or a Participating Entity, Contractor must provide an historic version of any Baseline Price List.

3. **Purchase Orders.**
There will be no minimum order requirements or charges to process an individual purchase order. The Participating Addendum number and the PO number must appear on all documents (e.g., invoices, packing slips, etc.). The Ordering Entity's purchase order constitutes a binding contract.

4. **Risk of Loss or Damage.**
The Purchasing Entity is relieved of all risks of loss or damage to the goods or equipment during periods of transportation, and installation by the Contractor and in the possession of the Contractor or their authorized agent.

5. **Payment Card Industry Data Security Standard and Cardholder Information Security.**
Contractor assures all of its Network Components, Applications, Servers, and Subcontractors (if any) comply with the Payment Card Industry Data Security Standard ("PCIDSS"). "Network Components" shall include, but are not limited to, Contractor's firewalls, switches, routers, wireless access points, network appliances, and other security appliances; "Applications" shall include, but are not limited to, all purchased and custom external (web) applications. "Servers" shall include, but are not limited to, all of Contractor's web, database, authentication, DNS, mail, proxy, and NTP servers. "Cardholder Data" shall mean any personally identifiable data associated with a cardholder, including, by way of example and without limitation, a cardholder's account number, expiration date, name, address, social security number, or telephone number.

Subcontractors (if any) must be responsible for the security of all Cardholder Data in its possession; and will only use Cardholder Data for assisting cardholders in completing a transaction, providing fraud control services, or for other uses specifically required by law. Contractor must have a business continuity program which conforms to PCIDSS to protect Cardholder Data in the event of a major disruption in its operations or in the event of any other disaster or system failure which may occur to operations; will continue to safeguard Cardholder Data in the event this Agreement terminates or expires; and ensure that a representative or agent of the payment card industry and a representative or agent of the Purchasing Entity shall be provided with full cooperation and access to conduct a thorough security review of Contractor's operations, systems, records, procedures, rules, and practices in the event of a security intrusion in order to validate compliance with PCIDSS.

6. **Foreign Outsourcing of Work.**
Upon request, the Contractor is required to provide information regarding the location of where services, data storage, and location of data processing under the Master Agreement will be performed.

7. **State Audits (Minn. Stat. § 16C.05, subd. 5).**
The books, records, documents, and accounting procedures and practices of the Contractor or other party, that are relevant to the Master Agreement or transaction are subject to examination by the contracting agency and either the Lead State's Legislative Auditor or State Auditor as appropriate for a minimum of six years after the end of the Master Agreement or transaction. The Lead State reserves the right to authorize delegate(s) to audit this Master Agreement and transactions.

8. **Certification of Nondiscrimination (in accordance with Minn. Stat. § 16C.053).**
If the value of this Contract, including all extensions, is $50,000 or more, Contractor certifies it does not engage in and has no present plans to engage in discrimination against Israel, or against persons or entities doing business in Israel, when making decisions related to the operation of the contractor's business. For purposes of this section, "discrimination" includes but is not limited to engaging in refusals to deal, terminating business activities, or other actions that are intended to limit commercial relations with Israel, or persons or entities doing business in Israel, when such actions are taken in a manner that in any way discriminates on the basis of nationality or national origin and is not based on a valid business reason.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

9. **Human Rights/Affirmative Action.**

The Lead State requires affirmative action compliance by its Contractors in accordance with Minn. Stat. § 363A.36 and Minn. R. 5000.3400 to 5000.3600.

a. Covered Contracts and Contractors. If the Contract exceeds $100,000 and the Contractor employed more than 40 full-time employees on a single working day during the previous 12 months in Minnesota or in the state where it has its principal place of business, then the Contractor must comply with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600.

b. Minn. R. 5000.3400-5000.3600 implement Minn. Stat. § 363A.36. These rules include, but are not limited to, criteria for contents, approval, and implementation of affirmative action plans; procedures for issuing certificates of compliance and criteria for determining a contractor's compliance status; procedures for addressing deficiencies, sanctions, and notice and hearing; annual compliance reports; procedures for compliance review; and contract consequences for noncompliance. The specific criteria for approval or rejection of an affirmative action plan are contained in various provisions of Minn. R. 5000.3400 5000.3600 including, but not limited to, parts 5000.3420-5000.3500 and parts 5000.3552 5000.3559.

c. Disabled Workers. Minn. R. 5000.3550 provides the Contractor must comply with the following affirmative action requirements for disabled workers.

AFFIRMATIVE ACTION FOR DISABLED WORKERS

(a) The Contractor must not discriminate against any employee or applicant for employment because of physical or mental disability in regard to any position for which the employee or applicant for employment is qualified. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified disabled persons without discrimination based upon their physical or mental disability in all employment practices such as the following: employment, upgrading, demotion or transfer, recruitment, advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

(b) The Contractor agrees to comply with the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.

(c) In the event of the Contractor's noncompliance with the requirements of this clause, actions for noncompliance may be taken in accordance with Minn. Stat. § 363A.36 and the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.

(d) The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices in a form to be prescribed by the commissioner of the Minnesota Department of Human Rights. Such notices must state the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified disabled employees and applicants for employment, and the rights of applicants and employees.

(e) The Contractor must notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of Minn. Stat. § 363A.36 of the Minnesota Human Rights Act and is committed to take affirmative action to employ and advance in employment physically and mentally disabled persons.

d. Consequences. The consequences of a Contractor's failure to implement its affirmative action plan or make a good faith effort to do so include, but are not limited to, suspension or revocation of a certificate of compliance by

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

the commissioner, refusal by the commissioner to approve subsequent plans, and termination of all or part of the Contract by the commissioner or the State.

e. Certification. The Contractor hereby certifies that it is in compliance with the requirements of Minn. Stat. § 363A.36, subd. 1 and Minn. R. 5000.3400-5000.3600 and is aware of the consequences for noncompliance. It is agreed between the parties that Minn. Stat. 363.36 and Minn. R. 5000.3400 to 5000.3600 are incorporated into any contract between these parties based upon this specification or any modification of it. A copy of Minn. Stat. § 363A.36 and Minn. R. 5000.3400 to 5000.3600 are available upon request from the contracting agency.

10. **Equal Pay Certification.**

If required by Minn. Stat. §363A.44, the Contractor must have a current Equal Pay Certificate prior to Contract execution. If Contractor's Equal Pay Certificate expires during the term of this Contract, Contractor must promptly re-apply for an Equal Pay Certificate with the Minnesota Department of Human Rights and notify the State's Authorized Representative once the Contractor has received the renewed Equal Pay Certificate. If Contractor claims to be exempt, the Lead State may require Contractor to verify its exempt status.

11. **Americans with Disabilities Act (ADA).**

Products provided under the Master Agreement must comply with the requirements of the Americans with Disabilities Act (ADA). The Contractor's catalog and other marketing materials utilized to offer products under the Master Agreement must state when a product is not in compliance. If any descriptive marketing materials are silent as to these requirements, the Contractor agrees that the customer can assume the product meets or exceeds the ADA requirements.

12. **Nonvisual Access Standards.**

Pursuant to Minn. Stat. § 16C.145, the Contractor shall comply with the following nonvisual technology access standards:

a. That the effective interactive control and use of the technology, including the operating system applications programs, prompts, and format of the data presented, are readily achievable by nonvisual means;

b. That the nonvisual access technology must be compatible with information technology used by other individuals with whom the blind or visually impaired individual must interact;

c. That nonvisual access technology must be integrated into networks used to share communications among employees, program participants, and the public; and

d. That the nonvisual access technology must have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

These standards do not require the installation of software or peripheral devices used for nonvisual access when the information technology is being used by individuals who are not blind or visually impaired.

13. **Accessibility Standards.**

Contractor acknowledges and is fully aware that the Lead State (Executive branch state agencies) has developed IT Accessibility Standard effective September 1, 2010. The standard entails, in part, the Web Content Accessibility Guidelines (WCAG) and Section 508 which can be viewed at: https://mn.gov/mnit/government/policies/accessibility/.

The Standards apply to web sites, software applications, electronic reports and output documentation, training delivered in electronic formats (including, but not limited to, documents, videos, and webinars), among others. As upgrades are made to the software, products, or subscriptions available through this Contract, the Contractor agrees to

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

develop functionality which supports accessibility. If any issues arise due to nonconformance with the above-mentioned accessibility Standards, the Contractor agrees to provide alternative solutions upon request at no additional charge to the State.

When updates or upgrades are made to the products or services available through this Contract, the Contractor agrees to document how the changes will impact or improve the product's or service's accessibility and usability. This documentation, upon request, must be provided to the Lead State in advance of the change, occurring within an agreed upon timeframe sufficient for the state to review the changes and either approve them or request a remediation plan from the Contractor. Contractor warrants that its Products comply with the above-mentioned accessibility Standards and agrees to indemnify, defend, and hold harmless the Lead State against any claims related to non-compliance of Contractor's Product with the above-mentioned accessibility Standards. If agreed-upon updates fail to improve the product or service's accessibility or usability as planned, the failure to comply with this requirement may be cause for contract cancellation or for the Lead State to consider the Contractor in default.

14. **Conflict Minerals.**
Contractor agrees to provide information upon request regarding adherence to the Conflict Minerals section of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Section 1502).

See: http://beta.congress.gov/111/bills/hr4173/111hr4173enr.pdf#page=838
http://www.sec.gov/news/press/2012/2012-163.htm

15. **Hazardous Substances.**
To the extent that the goods to be supplied by the Contractor contain or may create hazardous substances, harmful physical agents or infectious agents as set forth in applicable state and federal laws and regulations, the Contractor must provide Material Safety Data Sheets regarding those substances. A copy must be included with each delivery.

16. **Copyrighted Material Waiver.**
The Lead State reserves the right to use, reproduce and publish proposals in any manner necessary for State agencies and local units of government to access the responses, including but not limited to photocopying, State Intranet/Internet postings, broadcast faxing, and direct mailing. In the event that the response contains copyrighted or trademarked materials, it is the responder's responsibility to obtain permission for the Lead State to reproduce and publish the information, regardless of whether the responder is the manufacturer or reseller of the products listed in the materials. By signing its response, the responder certifies that it has obtained all necessary approvals for the reproduction and distribution of the contents of its response and agrees to indemnify, protect, save and hold the Lead State, its representatives and employees harmless from any and all claims arising from the violation of this section and agrees to pay all legal fees incurred by the Lead State in the defense of any such action.

17. **Publicity.**
The Contractor shall make no representations of the State's opinion or position as to the quality or effectiveness of the products or services that are the subject of the Master Agreement without the prior written consent of the State's Assistant Director or designee of Office of State Procurement. Representations include any publicity, including but not limited to advertisements, notices, press releases, reports, signs, and similar public notices.

18. **Performance While Dispute is Pending.**
Notwithstanding the existence of a dispute, the parties shall continue without delay to carry out all of their responsibilities under the Master Agreement that are not affected by the dispute. If a party fails to continue without delay to perform its responsibilities under the Master Agreement, in the accomplishment of all undisputed work, any additional cost incurred by the other parties as a result of such failure to proceed shall be borne by the responsible party.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

19. **Organizational Conflicts of Interest.**
An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons:

a. the Contractor is unable or potentially unable to render impartial assistance or advice to the State;

b. the Contractor's objectivity in performing the work is or might be otherwise impaired; or

c. the Contractor has an unfair competitive advantage.

The Contractor agrees that if an organizational conflict of interest is discovered after award, an immediate and full disclosure in writing shall be made to the Assistant Director of the Lead State's Department of Administration's Office of State Procurement that shall include a description of the action the Contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organizational conflict of interest is determined to exist, the Lead State may, at its discretion, cancel the Master Agreement. In the event the Contractor was aware of an organizational conflict of interest prior to the award of the Master Agreement and did not disclose the conflict to the Master Agreement Administrator, the Lead State may terminate the Master Agreement for default. The provisions of this clause shall be included in all subcontracts for work to be performed, and the terms "Contract," "Contractor," "Master Agreement", "Master Agreement Administrator" and "Contract Administrator" modified appropriately to preserve the State's rights.

20. **Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion**

a. Certification regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion – Lower Tier Covered Transactions. Instructions for certification:

1. By signing and submitting this proposal, the prospective lower tier participant [responder] is providing the certification set out below.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to whom this proposal [response] is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or had become erroneous by reason of changed circumstances.

4. The terms covered transaction, debarred, suspended, ineligible lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meaning set out in the Definitions and Coverages section of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this response that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction [subcontract equal to or exceeding $25,000] with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

6. The prospective lower tier participant further agrees by submitting this proposal that it will include this clause titled, “Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion – Lower Tier Covered Transaction,” without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from covered transactions, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the list of parties excluded from federal procurement and nonprocurement programs.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and debarment.

b. Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion – Lower Tier Covered Transactions.

1. The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

21. **Government Data Practices.**

The Contractor and the Lead State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (and where applicable, if the Lead State contracting party is part of the judicial branch, with the Rules of Public Access to Records of the Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by the Lead State to the Contractor and all data provided to the Lead State by the Contractor. In addition, the Minnesota Government Data Practices Act applies to all data created, collected, received, stored, used, maintained, or disseminated by the Contractor in accordance with the Master Agreement that is private, nonpublic, protected nonpublic, or confidential as defined by the Minnesota Government Data Practices Act, Ch. 13 (and where applicable, that is not accessible to the public under the Rules of Public Access to Records of the Judicial Branch).

In the event the Contractor receives a request to release the data referred to in this article, the Contractor must immediately notify the Lead State. The Lead State will give the Contractor instructions concerning the release of the data to the requesting party before the data is released. The civil remedies of Minn. Stat. § 13.08, apply to the release of the data by either the Contractor or the Lead State.

The Contractor agrees to indemnify, save, and hold the Lead State, its agent and employees, harmless from all claims arising out of, resulting from, or in any manner attributable to any violation of any provision of the Minnesota

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Government Data Practices Act (and where applicable, the Rules of Public Access to Records of the Judicial Branch), including legal fees and disbursements paid or incurred to enforce this provision of the Master Agreement. In the event that the Contractor subcontracts any or all of the work to be performed under the Master Agreement, the Contractor shall retain responsibility under the terms of this article for such work.

22. **Survivability.**
Certain rights and duties of the Lead State and Contractor will survive the expiration or cancellation of the RFP and resulting Master Agreement. These rights and duties include but are not limited to paragraphs: Indemnification; Limitations of Liability; State Audits; Government Data Practices; Governing Law and Venue; Publicity; and Administrative Fees.

23. **Severability.**
If any provision of the Master Agreement, including items incorporated by reference, is found to be illegal, unenforceable, or void, then both the Lead State and the Contractor shall be relieved of all obligations arising under such provisions. If the remainder of the Master Agreement is capable of performance it shall not be affected by such declaration or finding and shall be fully performed.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit C: Requirements

1. **Contractor Verification.**

Contractor must be a manufacturer of a Product in the Band(s) it is awarded a Master Agreement. "Re-branding" a product that is manufactured by another company does not meet this requirement. If the Contractor ceases production, sells or assigns their manufacturing to another vendor, or otherwise no longer manufactures a product during the life of the Master Agreement the Lead State reserves the right to terminate the Contractor's Master Agreement.

2. **Warranty and Maintenance.**

Contractor must ensure warranty service and maintenance for all equipment, including third party products provided. The Contractor must facilitate the Manufacturer or Publisher warranty and maintenance of third party products furnished through the Master Agreement. The Contractor shall provide the warranty service and maintenance for equipment and all peripherals on the Master Agreement.

3. **Website.**

Contractor must develop and maintain a URL to a web site specific to the awarded Master Agreement. Contractor's Master Agreement website must offer twenty-four (24) hours per day, seven (7) days per week availability, except for regularly scheduled maintenance times. The website must be separate from the Contractor's commercially available (i.e., public) on-line catalog and ordering systems. No other items or pricing may be shown on the website without written approval from the Lead State

a. Mandatory Specifications:

- Designated Baseline Price List(s) (e.g., MSRP, List, or Education)
- Product and Service Schedule (PSS)
- Product specifications, pricing, and configuration aids for the major product categories proposed that can be used to obtain an on-line quote,
- Service options and service agreements available on the contract. Please refer to Paragraph 5.
- Contact information for order placement, service concerns (warranty and maintenance), problem reporting, and billing concerns
- Sales representatives for participating entities
- Links to environmental certification, including but not limited to take-back/recycling programs, EPEAT, Energy Star, etc.

b. Desirable Specifications:

- Purchase order tracking
- Information on accessibility and accessible products
- Signed Master Agreement
- Online ordering capability with the ability to remember multiple ship to locations (if applicable to product)
- List of approved partners, if applicable

Within 30 calendar days of the notice of intent to award a Master Agreement, Contractor must provide a sample URL of the Master Agreement webpage to the Lead State for review and approval. The Lead State will review and determine acceptability of the website format and data. If the information is determined to be unacceptable or incorrect, the Contractor will have 15 calendar days to provide revisions to the Lead State. After the Lead State approves the website, Contractor may not make material changes to the website without notifying the Lead State through the ARF process and receiving written approval of the changes.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

4. **Environmental Certifications.**
Contractor must include environmental or supply chain responsibility certifications and registrations for products sold through this Contract on their website. Contractor must provide these certifications and registrations for specific products to Participating Entities upon request.

5. **EPEAT Registration.**
Contractor agrees that applicable products offered that have EPEAT Standards provided under the Master Agreement must have achieved a minimum EPEAT Bronze registration. This requirement does not apply to Band 3.

Contractor may propose the addition of a product that has not yet achieved a minimum EPEAT Bronze registration. The Lead State, in its sole discretion may require Contractor to provide the following documentation to support the addition of the proposed product:

- A letter from the Green Electronics Council (GEC) on GEC's letterhead confirming that the verification process is underway; or
- A copy of Contractor's GEC contract, Conformity Assurance Board (CAB) contract, and a letter from Contractor's CAB stating that the relevant product has been registered with the CAB and that verification is underway.

The Lead State reserves the right to reject the inclusion of such product, or if approved, require Contractor to remove the product at a later date if the product does not achieve a minimum EPEAT Bronze registration. The Contractor must remove any products that subsequently exit the verification process without achieving EPEAT Bronze or greater from the Master Agreement.

6. **Third-Party Products.**
Some products offered may be manufactured by a third party. Contractor, however, must provide or facilitate the warranty service and maintenance for all Third-Party Products on the Master Agreement either directly or pass-through from the manufacturer. Contractor may not offer products manufactured by another Contractor holding a Minnesota NASPO ValuePoint Master Agreement for Computer Equipment without approval from the Lead State. Warranty for third-party products must be provided by the Contractor. Warranty documents for products manufactured by a third party are preferred to be delivered to the Participating Entity with the products. Contractor can only offer Third-Party Products in a Band they have been awarded.

Third-Party Products are intended to enhance or supplement a Contractor's own product line, and are not intended to represent more than a third of Contractor's total sales under this Master Agreement. The Lead State may limit the sale of Third-Party Products through the Master Agreement during the life of the Master Agreement should Third-Party Product sales be determined to consistently exceed one third of the total sales under this Master Agreement. Such limitation may take the form of any action the Lead State so chooses, up to and including non-renewal or cancellation of the Master Agreement.

7. **Partner Utilization.**
If utilizing partners, the Contractor is responsible for the partners providing products and services, as well as warranty service and maintenance for equipment the partner provides. Participating Entities have the option of utilizing partners. Contractor must provide a Participating Entity a copy of its plan for partner utilization upon request. Contractor must make available a list of approved partners for each Participating Entity. Participating Entities must approve specific Partners as outlined within the relevant Participating Addendum, and only partners approved by the Participating Entity may be deployed. The Participating Entity will define the process to add and remove partners in their Participating Addendum.

8. **2019 National Defense Authorization Act, Section 889(f)(3).**
Under the 2019 National Defense Authorization Act, Section 889(f)(3), the US military is prohibited from purchasing video surveillance and telecommunications equipment from certain Chinese-owned technology firms. While US state are

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

not subject to this act, there is increasing concern for the security of state data. Contractor certifies for the term of this Master Agreement that it is not subject to laws, rules, or policies potentially requiring disclosure of, or provision of access to, customer data to foreign governments or entities controlled by foreign governments, and that Contractor's Products do not contain, include, or utilize components or services supplied by any entity subject to the same. Contractor also certifies that its Products do not contain, include, or utilize any covered technology prohibited under Section 889 of the National Defense Authorization Act, as amended.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Pricing Schedule

Attached and incorporated into this Master Agreement as Exhibit D is the Price Schedule.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

NASPO ValuePoint Computer Equipment (2023-2028)
CONTROL SET

Master Agreement: 23004
Contractor Name: Dell Marketing, LP

Awarded Bands:

x Band 1: Personal Computing Devices (Windows)
x Band 2: Personal Computing Devices (Non-Windows)
x Band 3: Servers and Storage

Band	Category Code	Category Description	Discount off Baseline List
1	1B	Band 1 - Minimum Discount	18.0%
1	1T	Band 1 - Third Party Product Minimum Discount	5.5%
2	2B	Band 2 - Minimum Discount	18.0%
2	2T	Band 2 - Third Party Product Minimum Discount	5.5%
3	3B	Band 3 - Minimum Discount	18.0%
3	3T	Band 3 - Third Party Product Minimum Discount	5.5%
	S-1	Standalone Services	4.0%
	S-2	Warranty Services	4.0%
	S-3	Training and Other Professional Services	4.0%

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

Discount Structure

Master Agreement: 23004
Contractor Name: Dell Marketing, LP
Baseline Price List: Posted on Contractor's dedicated NASPO ValuePoint website

Band 1: Personal Computer Equipment (Windows OS)

Band	Category Code	Category Description	Discount off Baseline List
1	**1B**	**Band 1 - Minimum Discount**	**18.0%**
1	1B-1	Desktops - Alienware, Inspiron, Vostro, XPS	0.5%
1	1B-2	Notebooks - Alienware, Inspiron, Vostro, XPS	2.5%
1	1B-3	Projectors/Monitors/Other Electronics	2.5%
1	1B-4	Displays	2.5%
1	1B-5	Imaging	2.5%
1	1B-6	Dell Branded - Printer accessories, parts, and toner	1.5%
1	1B-7	Spare Parts related to Band 1	0.5%
1	1B-8	Customer Kits	15.0%
1	1B-9	Ready to Ship configurations	4.0%
1	**1T**	**Band 1 - Third Party Product Minimum Discount**	**5.5%**
1	1T-1	Selected Third Party - Software and Peripherals	0.5%

Band 2: Personal Computer Equipment (Non-Windows OS)

Band	Category Code	Category Description	Discount off Baseline List
2	**2B**	**Band 2 - Minimum Discount**	**18.0%**
2	2B-1	Commercial Chromebooks	15.0%
2	2B-2	Consumer Chromebooks	15.0%
2	2B-3	Projectors/Monitors/Other Electronics	2.5%
2	2B-4	Displays	2.5%
2	2B-5	Imaging	2.5%
2	2B-6	Dell Branded - Printer accessories, parts, and toner	1.5%
2	2B-7	Spare Parts related to Band 2	0.5%
2	2B-8	Customer Kits	15.0%
2	2B-9	Ready to Ship configurations	4.0%
2	**2T**	**Band 2 - Third Party Product Minimum Discount**	**5.5%**
2	2T-1	Selected Third Party - Software and Peripherals (Non-discountable)	0.5%

Band 3: Servers and Storage

Band	Category Code	Category Description	Discount off Baseline List
3	**3B**	**Band 3 - Minimum Discount**	**18.0%**
3	3B-1	Spare Parts related to Band 3	0.5%
3	3B-2	Customer Kits	15.0%
3	**3T**	**Band 3 - Third Party Product Minimum Discount**	**5.5%**
3	3T-1	Selected Third Party - Software and Peripherals	0.5%

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

Volume-Based Discounts

Master Agreement: 23004
Contractor Name: Dell Marketing, LP

Bands 1 & 2

1. Per Transaction Multiple Unit Discount(s)

Contractor provides a contractual volume discount program as follows based on dollars in a single purchase order or combination of purchase orders submitted at one time by a Purchasing Entity, or multiple entities conducting a cooperative purchase.

Min $ Single Transaction	Max $ Single Transaction	Per Transaction Multiple Unit Discount
$100,000.00	$199,999.99	1.0%
$200,000.00	$399,999.99	2.0%
$400,000.00	$599,999.99	4.0%
$600,000.00	$999,999.99	6.0%
$1,000,000.00	No Maximum	8.0%

Note: Per Transaction Multiple Unit Discount does not apply to Category Exceptions, 3rd party products, services, and special promotional offers

2. Cumulative Discount(s)

Contractor provides a cumulative volume discount as follows based on dollars resulting from the cumulative purchases by all purchases made by Purchasing Entities for the duration of the Master Agreement.

Threshold	Discount Level
Up to 2B	0.0%
$2B to $4B	1.0%
$4B to $6B	2.0%
$6B to $8B	3.0%
$8B to $10B	4.0%
Greater than $10B	5.0%

Note: Cumulative Discount does not apply to Category Exceptions, 3rd party products, services, and special promotional offers

3. Other Discount(s)

none

Band 3

1. Per Transaction Multiple Unit Discount(s)

Contractor provides a contractual volume discount program as follows based on dollars in a single purchase order or combination of purchase orders submitted at one time by a Purchasing Entity, or multiple entities conducting a cooperative purchase.

Min $ Single Transaction	Max $ Single Transaction	Per Transaction Multiple Unit Discount
$250,000.00	$499,999.99	1.0%
$500,000.00	$999,999.99	2.0%
$1,000,000.00	$1,499,999.99	4.0%
$1,500,000.00	$1,999,999.99	6.0%
$2,000,000.00	No Maximum	8.0%

Note: Per Transaction Multiple Unit Discount does not apply to Category Exceptions, 3rd party products, services, and special promotional offers.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

2. Cumulative Discount(s)

Contractor provides a cumulative volume discount as follows based on dollars resulting from the cumulative purchases by all purchases made by Purchasing Entities for the duration of the Master Agreement.

Column1	Discount Level
Up to 2B	0.0%
$2B to $4B	1.0%
$4B to $6B	2.0%
$6B to $8B	3.0%
$8B to $10B	4.0%
Greater than $10B	5.0%

Note: Cumulative Discount does not apply to Category Exceptions, 3rd party products, services, and special promotional offers.

3. Other Discount(s)

Additional discount(s) available.

none

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

Master Agreement: 23004
Contractor Name: Dell Marketing, LP

Each Purchasing Entity will determine if and how services will be offered in the Participating

Travel for Services will be negotiated with each Participating Entity in the Participating Addendum.

All Awarded Bands		
Category Code	**Description of Service**	**Percent Discount**
S-1	Standalone Services	4.0%
S-2	Warranty Services	4.0%
S-3	Training and Other Professional Services	4.0%

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

Master Agreement: 23004
Contractor Name: Dell Marketing, LP

All Awarded Bands

Optional: Lease Rates

Dell Financial Services (DFS') payment solutions offer flexible end-of term options designed to suit each entity's unique needs. Payment terms are generally from 24 through 60 months and are tailored to match the essential useful life of the equipment to the payment term. Payments can be billed monthly, quarterly, semi-annually or annually.

DFS payment solution rates are adjusted quarterly in accordance with a formula based on fluctuations in treasury notes. Our rates are a function of several factors including estimates of future residual values, prevailing interest rates, borrowing costs, general and administrative expenses, and solution structure. Once a payment schedule has commenced, the rate remains constant for the term of the schedule.

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit D: Price Schedule

Prompt Payment Discount

Master Agreement: 23004
Contractor Name: Dell Marketing, LP

All Awarded Bands

		in 30
		in 15, Net 30
		in 10, Net 30
X		Net 30
	Other (specify):	

DocuSign Envelope ID: F019BE07-AEF0-4A14-B979-8BB85953FE52

Exhibit E: Contractor Terms and Conditions

Attached by reference as Exhibit E are the following Contractor document(s):

- **Software Licenses.** Customer's rights to use the Software delivered by Supplier are governed by the terms of the applicable end-user license agreement. Unless different terms have been agreed between the parties, the terms posted on www.dell.com/eula (the "EULA") shall apply. Supplier will provide a hard copy of the applicable terms upon request. Unless expressly otherwise agreed, microcode, firmware or operating system software required to enable the Equipment with which it is shipped to perform its basic or enhanced functions, is licensed for use solely on such Equipment.

- **Dell Return Policy.** Customer may return Products to Supplier pursuant to the return policy at www.dell.com/returnspolicy.

- **Equipment Warranty.** Unless provided otherwise in a Schedule, additional terms governing the limited warranties for Equipment are found at https://www.dell.com/learn/us/en/uscorp1/terms-of-sale-commercial-and-public-sector-warranties?c=us&l=en&s=corp or in the applicable documentation or Product Notice for the specific Equipment.

- **Product- and Service-Specific Terms.** Scope and details of Services and Product-specific terms are specified in the applicable standard service description that is attached to or referred in a Schedule or Quote, or is made available through the then-current Supplier website for product- or service-specific terms, currently located at www.dell.com/offeringspecificterms. Such standard descriptions are from time to time referred to as "Service Description(s)", "Product Notices" or "Service Briefs." The version of the applicable document that is effective as of the date of the applicable Quote, shall be deemed incorporated into the Order. Scope and details of customized Professional Services not covered by such a standard description shall be documented in a mutually agreed Statement of Work ("SOW").

These Contractor terms and conditions are being provided for **informational purposes only**. They are intended to be negotiated by Contractor and a Participating Entity as part of a Participating Addendum, or by Contractor and a Purchasing Entity as part of an Order, and shall apply only as agreed to in writing by the parties. Unless such terms are expressly accepted in writing, terms in the following document(s) that derogate the application to a Purchasing Entity of a corresponding term in this Master Agreement or applicable Participating Addendum shall be deemed void.

Your Quote is ready.

Your personalized Quote is now available for purchase.

Complete your order through our secure online checkout before your Quote expires.

Order Now

Quote Name:	**Dell Pro Slim Plus QBS1250 + Dell Pro 5 16**	Sales Rep	Kc Dudley
Quote No.	**3000206900867.1**	Phone	1(800) 4563355
Total	**$130,205.74**	Email	Kc.Dudley@dell.com
Customer #	1264342	**Billing To**	ACCOUNTS PAYABLE CITY OF REDLANDS P O BOX 3005 REDLANDS, CA 92373-1505
Quoted On	Sep. 21, 2026		
Expires by	Oct. 21, 2026		
Contract Name	Dell NASPO Computer Equipment PA - California		
Contract Code	C000001115143		
Customer Agreement #	23026 / 7-23-70-55-01		
Deal ID	31668693		

Message from your Sales Rep

If you are ready to place your order, you can click the order now button. If you need to make any changes you can call me directly at 512-720-7033 or e-mail me at kc.dudley@dell.com

Regards,
Kc Dudley

Shipping Group

Shipping To

RECEIVING DEPT
CITY OF REDLANDS
1270 W PARK AVE
PERSONNEL DEPT
REDLANDS, CA 92373-8112
(714) 798-7525

Shipping Method

Standard Delivery

Product	Unit Price	Quantity	Subtotal
Dell Pro Slim Plus QBS1250	**$1,535.07**	**50**	**$76,753.50**
Dell PRO 5 16 P516260	**$1,923.75**	**22**	**$42,322.50**
Dell Pro Thunderbolt 4 Dock WD25TB4	**$209.99**	**10**	**$2,099.90**

Dell Marketing LP. U.S. only. Dell Marketing LP. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682

Subtotal:	**$121,175.90**
Shipping:	**$0.00**
Environmental Fee:	**$110.00**
Non-Taxable Amount:	**$19,344.60**
Taxable Amount:	**$101,941.30**
Estimated Tax:	**$8,919.84**
Total:	**$130,205.74**

Special pricing may be available for qualified customers. Please contact your DFS Sales Representative for details.

Shipping Group Details

Shipping To

RECEIVING DEPT
CITY OF REDLANDS
1270 W PARK AVE
PERSONNEL DEPT
REDLANDS, CA 92373-8112
(714) 798-7525

Shipping Method

Standard Delivery

	Unit Price	Quantity	Subtotal
Dell Pro Slim Plus QBS1250	**$1,535.07**	**50**	**$76,753.50**

Estimated delivery if purchased today:
Oct. 05, 2026
Contract # C000001115143
Customer Agreement # 23026 / 7-23-70-55-01

Description	SKU	Tax Type	Unit Price	Quantity	Subtotal
Intel(R) Core(TM) Ultra 7 265 (13 TOPS NPU, 20 cores, up to 5.3GHz)	338-CRZM	T	-	50	-
Windows 11 Pro	619-BBQD	T	-	50	-
16GB: 1 x 16GB, DDR5, up to 5600 MT/s, non-ECC	370-BCWX	T	-	50	-
512GB SSD	400-BSWY	T	-	50	-
Screw for SSD	773-BBBC		-	50	-
Integrated Graphics	490-BKSX		-	50	-
No Wireless LAN Card	555-BLXL		-	50	-
Internal speaker	520-BBKW		-	50	-
No Additional Add In Cards	382-BBHX		-	50	-
Dell Pro Slim Plus QBS1250 with 260W PSU	329-BKSP	T	-	50	-
Dell Pro 5 Keyboard and Mouse - KM526 - Black - US English - DAO	580-BDFZ	T	-	50	-
Mouse included with Keyboard	570-AADI		-	50	-
ENERGY STAR Qualified	387-BBLW		-	50	-
System Power Cord C13 (Philipine/TH/US)	450-AAOJ		-	50	-
Documentation	340-DNBV		-	50	-
Watch Dog SRV	379-BFYR		-	50	-
Quick Start Guide	340-DTTZ		-	50	-
US/Canada Battery Warning Label	389-FKHG		-	50	-
Trusted Platform Module (Discrete TPM Enabled)	329-BBJL		-	50	-
Shipping Material (DAO)	340-DTSR		-	50	-
Shipping Label	389-BBUU		-	50	-
DAO Regulatory label for 260W PSU	389-FJYR		-	50	-
Driver/APP for IRST	658-BFTS		-	50	-
Intel(R) Core(TM) Ultra 7 vPro Processor Label	389-FJVS		-	50	-
Desktop BTO Standard shipment	800-BBIO		-	50	-
Dell Pro Slim Plus QBS1250	210-BPPM	T	-	50	-
No Optical Drive	429-BBCH		-	50	-
Intel vPro(R) Enterprise	631-BCBN	T	-	50	-

Dell Marketing LP. U.S. only. Dell Marketing LP. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682

EPEAT Silver with Climate+	379-BDTO		-	50	-
No Additional Add In Cards	382-BBHX		-	50	-
No Additional Network Card Selected (Integrated NIC included)	555-BBJO		-	50	-
No Additional Video Ports	492-BCKH		-	50	-
No Media Card Reader	379-BBHM		-	50	-
NO RAID	817-BBBN		-	50	-
English, French, Spanish, Brazilian Portuguese	619-BBPD		-	50	-
CMS Software not included	632-BBBJ		-	50	-
Custom Configuration	817-BBBB		-	50	-
No Hazardous Locations Certification	340-ACQQ		-	50	-
No Hard Drive Bracket	575-BBKX		-	50	-
Dell Limited Hardware Warranty Plus Service	717-8784	T	-	50	-
ProSupport: 7x24 Technical Support, 5 Years	717-8823	N	-	50	-
ProSupport: Next Business Day Onsite, 5 Years	717-8827	N	-	50	-
Thank you choosing Dell ProSupport. For tech support, visit //support.dell.com/ProSupport	989-3449		-	50	-
Activate Your Microsoft 365 For A 30 Day Trial	630-ABBT		-	50	-
Dell Pro Slim Plus QBS1250	658-BFVK		-	50	-

	Unit Price	**Quantity**	**Subtotal**
Dell PRO 5 16 P516260	**$1,923.75**	**22**	**$42,322.50**

Estimated delivery if purchased today:
Oct. 08, 2026
Contract # C000001115143
Customer Agreement # 23026 / 7-23-70-55-01

Description	SKU	Tax Type	Unit Price	Quantity	Subtotal
Dell Pro 5 16 (P516260) CTO Base	210-BWBR	T	-	22	-
Dell Pro 5 16 (P516260) CTO Base	631-BCPQ		-	22	-
Series 3 Intel(R) Core(TM) Ultra 7 365 vPro(R) (8 cores, up to 4.8 GHz, 49 TOPS NPU)	379-BGRK	T	-	22	-
Windows 11 Pro, Copilot+ PC	619-BBGJ	T	-	22	-
Aluminum (Top Cover, Palm-rest, Bottom Cover)	321-BNCH	T	-	22	-
16 GB: 1 x 16 GB, DDR5, 5600 MT/s, single channel	370-BCNG	T	-	22	-
Integrated Intel(R) Graphics, 4Xe with Intel(R) Core(TM) Ultra 7 365, vPro(R) CPU	338-CVQS		-	22	-
512 GB SSD	400-BVND	T	-	22	-
Intel(R) Wi-Fi 7 BE211, Qualified against Bluetooth(R) Core 6.0 wireless Card	555-BNPW	T	-	22	-
16", WUXGA (1920x1200), Touch, 400nit, 62.5% sRGB, Anti-Glare, FHD+IR Cam	391-BKXW	T	-	22	-
FHD RGB HDR + IR Camera, 1080p at 30 fps, Presence Detection, TNR, Camera Shutter, Microphone	319-BBMM		-	22	-
English (US) Mini-LED backlit keyboard with numeric keypad	583-BPHR	T	-	22	-
No Fingerprint Reader, No Smart Card Reader	346-BNCF	T	-	22	-
Intel(R) vPro(R) Enabled	631-BCMY	T	-	22	-

3-cell, 57 Wh, ExpressCharge Boost capable battery, 1-yr limited hardware warranty	451-BDQQ	T	-	22	-
65W USB-C AC Adapter	492-BFFW		-	22	-
E4 Power Cord 1M for US	470-BCXK		-	22	-
Single-System Packaging (Vertical Box)	340-FBDH		-	22	-
English, French, Spanish, Brazilian Portuguese	619-BBPD		-	22	-
Intel(R) BE211 WLAN Driver	555-BNSV		-	22	-
Quick Reference Card	340-DZXG		-	22	-
Documentation	340-DNBV		-	22	-
ENERGY STAR Qualified	387-BBLW		-	22	-
Series 3 Intel(R) Core(TM) Ultra 7 vPro(R) Processor Label	389-FRCX		-	22	-
Aluminum (Top Cover, Palm-rest, Bottom Cover), SODIMM, WLAN	321-BMZK	T	-	22	-
EPEAT Gold with Climate+	379-BGNT		-	22	-
Intel(R) Connectivity Performance Suite	640-BBTL		-	22	-
Thermal Pad 2230 SSD	575-BCWP		-	22	-
Custom Configuration	817-BBBB		-	22	-
ProSupport: Next Business Day Onsite, 1 Year	714-0174	N	-	22	-
ProSupport: Next Business Day Onsite, 4 Year Extended	714-0205	N	-	22	-
ProSupport: 7x24 Technical Support, 5 Years	714-0217	N	-	22	-
Dell Limited Hardware Warranty	714-0313	T	-	22	-
Dell Limited Hardware Warranty Extended Year(s)	975-3461		-	22	-
Thank you choosing Dell ProSupport. For tech support, visit //support.dell.com/ProSupport	989-3449		-	22	-
Activate Your Microsoft 365 For A 30 Day Trial	630-ABBT		-	22	-
Dell Additional SW - Dell Pro Laptop	658-BFVB		-	22	-
Foxit PDF Editor with AI Assistant	634-CZWL	T	-	22	-
CyberLink Media Player with PowerDVD 24	634-BWZO	T	-	22	-

			Unit Price	Quantity	Subtotal
Dell Pro Thunderbolt 4 Dock WD25TB4			**$209.99**	**10**	**$2,099.90**

Estimated delivery if purchased today:
Sep. 24, 2026
Contract # C000001115143
Customer Agreement # 23026 / 7-23-70-55-01

Description	SKU	Tax Type	Unit Price	Quantity	Subtotal
Dell Pro Thunderbolt 4 Dock - WD25TB4	210-BTMR	T	-	10	-
Dell Limited Hardware Warranty	718-2132	T	-	10	-
Advanced Exchange Service 3 Years	718-2133		-	10	-

Subtotal:	**$121,175.90**
Shipping:	**$0.00**
Environmental Fee:	**$110.00**
Estimated Tax:	**$8,919.84**
Total:	**$130,205.74**

Dell Marketing LP. U.S. only. Dell Marketing LP. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682

Important Notes

Terms of Sale

This Quote will, if Customer issues a purchase order for the quoted items that is accepted by Supplier, constitute a contract between the entity issuing this Quote ("Supplier") and the entity to whom this Quote was issued ("Customer"). Unless otherwise stated herein, pricing is valid for Thirty (30) days from the date of this Quote. All products, pricing, and other information are based on the latest information available and are subject to change for any reason. Taxes and/or freight charges listed on this Quote are only estimates. The final amounts shall be stated on the relevant invoice. Additional freight charges will be applied if Customer requests expedited shipping. Please indicate any tax exemption status on your purchase order and send your tax exemption certificate to Tax_Department@dell.com or ARSalesTax@emc.com, as applicable.

Prices and/or discounts, as applicable, are subject to change: (i) in the event of industry-wide shortages in materials or resources, increases in the cost of manufacturing, currency fluctuations, changes to government charges or tariffs, or other factors outside Supplier's control; (ii) in the event of structural or significant changes in the way Supplier develops its pricing and/or discounting strategy; (iii) if Customer requests changes to Supplier's planned delivery date; or (iv) if Customer materially breaches its commitments under this Quote. If such changes occur, pricing may be adjusted and/or purchase orders may be cancelled by Supplier until the date of shipment, even after an order has been placed. Supplier will give Customer as much notice of these changes as is reasonably practicable under the circumstances. Supplier also reserves the right to cancel this Quote and Customer purchase orders arising from pricing errors and/or Customer changes to Supplier's planned delivery date.

Entire Agreement – This Quote, including the Governing Terms, Schedules, any Offering Specific Terms incorporated by reference and each Order, comprises the complete statement of the agreement of the Parties regarding the subject matter thereof, and may be amended only by written agreement. Terms on any Order or any term or condition on a Customer form have no legal effect and do not modify or supplement these Terms of Sale.

Governing Terms: This Quote is subject to: (a) a separate written agreement between Customer or Customer's affiliate and Supplier or a Supplier´s affiliate to the extent that it expressly applies to the products and/or services in this Quote or, to the extent there is no such agreement, to the applicable set of Dell's Terms of Sale (available at www.dell.com/terms or www.dell.com/oemterms), or for cloud/as-a-Service offerings, the applicable cloud terms of service (identified on the Offer Specific Terms referenced below); and (b) the terms referenced herein (collectively, the "Governing Terms"). Different Governing Terms may apply to different products and services on this Quote. The Governing Terms apply to the exclusion of all terms and conditions incorporated in or referred to in any documentation submitted by Customer to Supplier.

Supplier Software Licenses and Services Descriptions: Customer's use of any Supplier software is subject to the license terms accompanying the software, or in the absence of accompanying terms, the applicable terms posted on www.Dell.com/eula. Descriptions and terms for Supplier-branded standard services are stated at www.dell.com/servicecontracts/global or for certain infrastructure products at www.dellemc.com/en-us/customer-services/product-warranty-and-service-descriptions.htm.

Offer-Specific, Third Party and Program Specific Terms: Customer's use of third-party software is subject to the license terms that accompany the software. Certain Supplier-branded and third-party products and services listed on this Quote are subject to additional, specific terms stated on www.dell.com/offeringspecificterms ("Offer Specific Terms").

In case of Resale only: Should Customer procure any products or services for resale, whether on standalone basis or as part of a solution, Customer shall include the applicable software license terms, services terms, and/or offer-specific terms in a written agreement with the end-user and provide written evidence of doing so upon receipt of request from Supplier.

In case of Financing only: If Customer intends to enter into a financing arrangement ("Financing Agreement") for the products and/or services on this Quote with Dell Financial Services LLC or other funding source pre-approved by Supplier ("FS"), Customer may issue its purchase order to Supplier or to FS. If issued to FS, Supplier will fulfill and invoice FS upon confirmation that: (a) FS intends to enter into a Financing Agreement with Customer for this order; and (b) FS agrees to procure these items from Supplier. Notwithstanding the Financing Agreement, Customer's use (and Customer's resale of and the end-user's use) of these items in the order is subject to the applicable governing agreement between Customer and Supplier, except that title shall transfer from Supplier to FS instead of to Customer. If FS notifies Supplier after shipment that Customer is no longer pursuing a Financing Agreement for these items, or if Customer fails to enter into such Financing Agreement within 120 days after shipment by Supplier, Customer shall promptly pay the Supplier invoice amounts directly to Supplier.

Customer represents that this transaction does not involve: (a) use of U.S. Government funds; (b) use by or resale to the U.S. Government; or (c) maintenance and support of the product(s) listed in this document within classified spaces. Customer further represents that this transaction does not require Supplier's compliance with any statute, regulation or information technology standard applicable to a U.S. Government procurement.

For certain products shipped to end users in California, a State Environmental Fee will be applied to Customer's invoice. Supplier encourages customers to dispose of electronic equipment properly.

Electronically linked terms and descriptions are available in hard copy upon request.

City Council **AGENDA ITEM NO. I8.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve Final Map for Tract No. 20402 prepared and submitted by TH Canyon Ranch Loma Linda LLC located at the northeast corner of Nevada Street and San Timoteo Canyon Road and approximately 400 feet south of Bermudez Street (Development Services Director Reilly)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council approve the Final Map for Tract No. 20402.

RECOMMENDATION:

Staff recommends that City Council approve the Final Map for Tract No. 20402.

DISCUSSION:

The applicant is requesting approval of the Final Map for Tract No. 20402. On December 12, 2023, the Planning Commission approved Tentative Tract Map No. 20402 to subdivide a 21.6-acre vacant parcel into 27 lots for future single-family residential development, with a minimum lot size of 20,000 square-feet each, and seven lettered lots (for open space, landscaping, and water quality treatment purposes). The project site is located at the northeast corner of Nevada Street and San Timoteo Canyon Road and approximately 400 feet south of Bermudez Street within the Agriculture (A-1) zoning district (APNs: 0293-141-38-0000 and 0293-132-01- 0000). Planning Commission Resolution No. 1636 approved the following project actions:

1. Adopted a Mitigated Negative Declaration;
2. Adopted the Socio-Economic Cost/Benefit Study;
3. Approved Tentative Tract Map No. 20402;
4. Commission Review and Approval No. 969; and
5. Approved Street Vacation No. 193.

The owner has complied with all conditions of approval for Tentative Tract Map 20402. The Final Map (Attachment A) has been reviewed by staff and the City's contracted Public Land Surveyor. The Subdivision Improvement Agreement (Attachment B) and appropriate financial securities including a faithful performance bond (Attachment C) and a labor and materials bond (Attachment D) have been prepared based on the project engineer's estimated construction costs. These securities will ensure that off-site improvements are installed when project development begins.

ALTERNATIVES:

City Council may deny the Final Map for Tract No. 20402.

STRATEGIC PLAN:

Not applicable.

SUBMITTED BY:
Sean Reilly, Development Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Rosemary Montoya, Associate Planner

FISCAL IMPACT

Fiscal Year: 26-27

Revenue Generating: N/A

Amount:

Budgeted Y/N:

Account No.:

Additional Appropriation Required:

Discussion:

No impact to the General Fund. The applicant paid the applicable application filing fee.

Attachments

Attachment_A_-_Final_Map_No_20402.pdf
Attachment_B_-_Subdivision_Improvement_Agreement.pdf
Attachment_C-_Faithful_Performance_Bond.pdf
Attachment_D_-_Labor_and_Materials_Bond.pdf

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486 ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106 DATE OF SURVEY: NOVEMBER, 2023

OWNER'S STATEMENT

WE HEREBY STATE THAT WE ARE THE ONLY PARTIES HAVING ANY RECORD TITLE INTEREST IN THE LAND SUBDIVIDED AS SHOWN ON THIS MAP, AND WE CONSENT TO THE PREPARATION AND RECORDATION OF THIS FINAL MAP.

WE HEREBY DEDICATE TO THE CITY OF REDLANDS, WILDFLOWER WAY, EAGLE CREST ROAD, TIMBERLINE TRAIL AND SAN TIMOTEO CANYON ROAD FOR PUBLIC ROADS AND PUBLIC UTILITY PURPOSES, AS SHOWN ON THIS MAP.

WE ALSO HEREBY RESERVE, FOR THE USE AND BENEFIT OF LOTS 23 AND 24, AN EASEMENT OVER ALL OF LOT 'F' FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES, SHOWN AS EASEMENT (A) ON THIS MAP.

WE ALSO HEREBY RESERVE, FOR THE USE AND BENEFIT OF LOTS 11 AND 12, AN EASEMENT OVER ALL OF LOT 'G' FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES, SHOWN AS EASEMENT (B) ON THIS MAP.

WE ALSO HEREBY RESERVE TO OURSELVES, OUR HEIRS, AND ASSIGNS, FOR THE USE AND BENEFIT OF THE FUTURE HOMEOWNER'S ASSOCIATION, AN EASEMENT OVER ALL OF LOTS 'A' AND 'B' FOR STORM DRAIN PURPOSES, SHOWN AS EASEMENT (C) ON THIS MAP.

WE ALSO HEREBY RESERVE TO OURSELVES, OUR HEIRS, AND ASSIGNS, FOR THE USE AND BENEFIT OF THE FUTURE HOMEOWNER'S ASSOCIATION, LOT 'A' FOR BASIN PURPOSES, LOT 'B' FOR OPEN SPACE PURPOSES, LOTS 'C', 'D' AND 'E' ARE FOR LANDSCAPE PURPOSES, LOT 'F' FOR PRIVATE ACCESS PURPOSES FOR LOTS 23 AND 24 AND LOT 'G' FOR PRIVATE ACCESS PURPOSES FOR LOTS 11 AND 12.

KL LB BUY 4 LLC, A DELAWARE LIMITED LIABILITY COMPANY

BY: Ed Hadley

NAME: Ed Hadley

TITLE: Authorized Signatory

OPTIONEE

A MEMORANDUM OF OPTION AGREEMENT WITH TH CANYON RANCH LOMA LINDA LLC, A CALIFORNIA LIMITED LIABILITY COMPANY (OPTIONEE), BY DOCUMENT RECORDED JULY 29, 2024 AS DOCUMENT NO. 2024–0178086 OF OFFICIAL RECORDS.

TH CANYON RANCH LOMA LINDA LLC, A CALIFORNIA LIMITED LIABILITY COMPANY

BY: _____

NAME: RICHARD P. DOUGLASS

TITLE: AUTHORIZED SIGNATORY

NOTARY ACKNOWLEDGMENT

A NOTARY PUBLIC OR OTHER OFFICER COMPLETING THIS CERTIFICATE VERIFIES ONLY THE IDENTITY OF THE INDIVIDUAL WHO SIGNED THE DOCUMENT TO WHICH THIS CERTIFICATE IS ATTACHED, AND NOT THE TRUTHFULNESS, ACCURACY, OR VALIDITY OF THAT DOCUMENT.

STATE OF California)
COUNTY OF Orange)

ON July 28th, 2026, BEFORE ME, Marina Maree Kerner, NOTARY PUBLIC,
(INSERT NAME)

PERSONALLY APPEARED Richard P. Douglass,
WHO PROVED TO ME ON THE BASIS OF SATISFACTORY EVIDENCE TO BE THE PERSON(S) WHOSE NAME(S) IS/ARE SUBSCRIBED TO THE WITHIN INSTRUMENT AND ACKNOWLEDGED TO ME THAT HE/SHE/THEY EXECUTED THE SAME IN HIS/HER/THEIR AUTHORIZED CAPACITY(IES), AND THAT BY HIS/HER/THEIR SIGNATURE(S) ON THE INSTRUMENT THE PERSON(S), OR THE ENTITY UPON BEHALF OF WHICH THE PERSON(S) ACTED, EXECUTED THE INSTRUMENT.

I CERTIFY UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF CALIFORNIA THAT THE FOREGOING PARAGRAPH IS TRUE AND CORRECT.

WITNESS MY HAND.

Marina Maree Kerner — NAME PRINTED
Marina Maree Kerner — SIGNATURE OF OFFICER

MY COMMISSION NO: 2330122 MY COMMISSION EXPIRES March 17th, 2030

MY PRINCIPAL PLACE OF BUSINESS IS Orange COUNTY.

NOTARY ACKNOWLEDGMENT

A NOTARY PUBLIC OR OTHER OFFICER COMPLETING THIS CERTIFICATE VERIFIES ONLY THE IDENTITY OF THE INDIVIDUAL WHO SIGNED THE DOCUMENT TO WHICH THIS CERTIFICATE IS ATTACHED, AND NOT THE TRUTHFULNESS, ACCURACY, OR VALIDITY OF THAT DOCUMENT.

STATE OF ARIZONA)
COUNTY OF MARICOPA)

ON July 29th, 2026, BEFORE ME, Julie Gillett, NOTARY PUBLIC,
(INSERT NAME)

PERSONALLY APPEARED Ed Hadley,
WHO PROVED TO ME ON THE BASIS OF SATISFACTORY EVIDENCE TO BE THE PERSON(S) WHOSE NAME(S) IS/ARE SUBSCRIBED TO THE WITHIN INSTRUMENT AND ACKNOWLEDGED TO ME THAT HE/SHE/THEY EXECUTED THE SAME IN HIS/HER/THEIR AUTHORIZED CAPACITY(IES), AND THAT BY HIS/HER/THEIR SIGNATURE(S) ON THE INSTRUMENT THE PERSON(S), OR THE ENTITY UPON BEHALF OF WHICH THE PERSON(S) ACTED, EXECUTED THE INSTRUMENT.

I CERTIFY UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF ~~CALIFORNIA~~ ARIZONA THAT THE FOREGOING PARAGRAPH IS TRUE AND CORRECT.

WITNESS MY HAND.

Julie Gillett — NAME PRINTED
Julie Gillett — SIGNATURE OF OFFICER

MY COMMISSION NO: 635441 MY COMMISSION EXPIRES 08/05/2026

MY PRINCIPAL PLACE OF BUSINESS IS MARICOPA COUNTY.

SIGNATURE OMISSIONS

PURSUANT TO THE PROVISIONS OF SECTION 66436 (a)(3)(B) OF THE SUBDIVISION MAP ACT, THE SIGNATURES OF THE FOLLOWING OWNERS OF EASEMENTS AND/OR OTHER INTERESTS HAVE BEEN OMITTED, THE SUCCESSOR IN INTEREST IS NOT LOCATABLE AND SIGNATURE ARE IMPOSSIBLE TO OBTAIN:

H.H. DANIELS, HOLDER OF AN EASEMENT FOR PIPE LINES AND INCIDENTAL PURPOSES, RECORDED NOVEMBER 20, 1889 IN BOOK 106, PAGE 116 OF DEEDS.

H.H. DANIELS, HOLDER OF AN EASEMENT FOR PIPE LINES AND INCIDENTAL PURPOSES, RECORDED JUNE 12, 1890 IN BOOK 115, PAGE 158 OF DEEDS.

PACIFIC TELEPHONE AND TELEGRAPH COMPANY, HOLDER OF AN EASEMENT FOR POLE LINES AND INCIDENTAL PURPOSES, RECORDED DECEMBER 17, 1910 IN BOOK 470, PAGE 3 OF DEEDS.

SOUTHERN CALIFORNIA EDISON COMPANY, HOLDER OF AN EASEMENT FOR POLE LINES AND INCIDENTAL PURPOSES, RECORDED APRIL 2, 1912 IN BOOK 504, PAGE 235 OF DEEDS.

SOUTHERN CALIFORNIA EDISON COMPANY, HOLDER OF AN EASEMENT FOR UNDERGROUND ELECTRICAL SUPPLY SYSTEMS, COMMUNICATION SYSTEMS AND INCIDENTAL PURPOSES, RECORDED DECEMBER 26, 2025 AS DOCUMENT NO. 2025–0315274 OF OFFICIAL RECORDS.

SURVEYOR'S STATEMENT

THIS MAP WAS PREPARED BY ME OR UNDER MY DIRECTION AND IS BASED UPON A FIELD SURVEY IN CONFORMANCE WITH THE REQUIREMENTS OF THE SUBDIVISION MAP ACT AND LOCAL ORDINANCE AT THE REQUEST OF KL LB BUY 4 LLC, IN NOVEMBER 2023. I HEREBY STATE THAT ALL MONUMENTS SHOWN HEREON ARE OF THE CHARACTER AND OCCUPY THE POSITIONS INDICATED, OR THAT THEY WILL BE SET IN SUCH POSITIONS WITHIN 24 MONTHS OF RECORDATION, AND THAT SAID MONUMENTS ARE SUFFICIENT TO ENABLE THE SURVEY TO BE RETRACED, AND I HEREBY STATE THAT THIS TRACT MAP SUBSTANTIALLY CONFORMS TO THE APPROVED OR CONDITIONALLY APPROVED TENTATIVE MAP, IF ANY.

LICENSED LAND SURVEYOR — CHARLES J. MOORE — L.S. 9106 — STATE OF CALIFORNIA

CHARLES J. MOORE, L.S. 9106 — DATE: July 24, 2026

CITY ENGINEER'S STATEMENT

I HEREBY STATE THAT I HAVE EXAMINED THIS MAP, AND THAT THE SUBDIVISION SHOWN HEREON IS SUBSTANTIALLY THE SAME AS IT APPEARED ON THE TENTATIVE TRACT MAP AND ANY APPROVED ALTERATIONS THEREOF, AND THAT ALL OF THE PROVISIONS OF CHAPTER 2 OF THE SUBDIVISION MAP ACT AND THE CITY OF REDLANDS MUNICIPAL CODE HAVE BEEN COMPLIED WITH.

REGISTERED PROFESSIONAL ENGINEER — GOUTAM K. DOBEY — NO. C75646 — CIVIL — STATE OF CALIFORNIA

GOUTAM K. DOBEY, R.C.E. C75646 — DATE: 8/4/26
CITY ENGINEER, CITY OF REDLANDS

I AM SATISFIED SAID MAP IS TECHNICALLY CORRECT.

PROFESSIONAL LAND SURVEYOR — MITCHAL L. CASSEL — L.S. 7504 — STATE OF CALIFORNIA

MITCHAL L. CASSEL, L.S. 7504 — DATE: 8-4-26
CONTRACT SURVEYOR, CITY OF REDLANDS

CITY CLERK'S STATEMENT

I HEREBY STATE THAT THE CITY COUNCIL OF THE CITY OF REDLANDS, BY A MOTION DULY SECONDED AND PASSED, APPROVED THIS MAP ON THE _____ DAY OF _____, 20 _____ AND ACCEPTED THE DEDICATION OF WILDFLOWER WAY, EAGLE CREST ROAD, TIMBERLINE TRAIL AND SAN TIMOTEO CANYON ROAD FOR PUBLIC ROADS AND PUBLIC UTILITY PURPOSES.

JEANNE DONALDSON — DATE
CITY CLERK, CITY OF REDLANDS

ABANDONMENT NOTE

PURSUANT TO SECTIONS 66434 AND 66499.20.2 OF THE SUBDIVISION MAP ACT, THE APPROVAL AND RECORDATION OF THIS TRACT MAP CONSTITUTES ABANDONMENT OF THE FOLLOWING:

THAT PORTION OF SAN TIMOTEO CANYON ROAD AS DESCRIBED IN A ROAD DEED, RECORDED MARCH 13, 1891, IN BOOK 1, PAGE 108, OF DEEDS, LYING WITHIN THE BOUNDARY OF THIS TRACT MAP.

BOARD OF SUPERVISORS CERTIFICATE

I HEREBY CERTIFY THAT A BOND IN THE SUM OF $ _____ HAS BEEN EXECUTED AND FILED WITH THE BOARD OF SUPERVISORS OF SAN BERNARDINO COUNTY, STATE OF CALIFORNIA, CONDITIONED UPON PAYMENT OF ALL TAXES, (STATE, COUNTY, MUNICIPAL OR LOCAL) AND ALL SPECIAL ASSESSMENTS, COLLECTED AS TAXES, WHICH AT THE TIME OF FILING OF THIS MAP WITH THE SAN BERNARDINO COUNTY ASSESSOR–RECORDER–COUNTY CLERK, ARE A LIEN AGAINST SAID PROPERTY, BUT NOT YET PAYABLE; AND THAT THE SUBDIVIDER HAS FILED WITH ME A CERTIFICATE BY THE PROPER OFFICER GIVING HIS ESTIMATE OF THE AMOUNT OF SAID TAXES AND SPECIAL ASSESSMENTS; AND SAID BOND IS HEREBY ACCEPTED.

LYNNA MONELL
CLERK OF THE BOARD OF SUPERVISORS
SAN BERNARDINO COUNTY

BY: _____, DEPUTY DATED: _____

AUDITOR–CONTROLLER/TREASURER/TAX COLLECTOR'S CERTIFICATE

I HEREBY CERTIFY THAT ACCORDING TO THE RECORDS OF THE OFFICE, AS OF THIS DATE, THERE ARE NO LIENS AGAINST THE REAL PROPERTY SHOWN UPON THIS MAP FOR UNPAID STATE, COUNTY, MUNICIPAL, OR LOCAL TAXES, OR SPECIAL ASSESSMENTS COLLECTED AS TAXES, EXCEPT TAXES OR SPECIAL ASSESSMENTS NOT YET PAYABLE, ESTIMATED TO BE $ _____

ENSEN MASON
AUDITOR–CONTROLLER/TREASURER/TAX COLLECTOR
SAN BERNARDINO COUNTY

BY: _____ DEPUTY DATED: _____

SAN BERNARDINO COUNTY RECORDER'S CERTIFICATE

THIS MAP HAS BEEN FILED UNDER DOCUMENT NUMBER _____, O.R. THIS _____ DAY OF _____, 20____ AT _____, M. IN BOOK _____ OF TRACT MAPS AT PAGES _____, AT THE REQUEST OF _____ IN THE AMOUNT OF $ _____

JOSIE GONZALES
ASSESSOR–RECORDER–COUNTY CLERK
SAN BERNARDINO COUNTY

BY: _____
DEPUTY RECORDER

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.

PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106
DATE OF SURVEY: NOVEMBER, 2023

MONUMENT NOTES

SET LEAD, TACK, & TAG "LS 9106" FLUSH IN TOP OF CURB ON SIDE LOT LINES PROJECTED.

SET LEAD, TACK, & TAG "LS 9106" FLUSH IN TOP OF CURB FOR BCs, ECs, PCCs, PRCs, & CORNER CUTBACKS PROJECTED PERPENDICULAR OR RADIAL FROM CENTERLINE.

ALL MONUMENTS SHOWN AS "SET" SHALL BE SET IN ACCORDANCE WITH THE TERMS OF THE MONUMENTATION AGREEMENT FOR THIS MAP.

○ – INDICATES 1" IRON PIPE & TAG "LS 9106", FLUSH, OR SPIKE & WASHER "LS 9106", FLUSH, OR LEAD, TACK & TAG "LS 9106" TO BE SET, FLUSH.

● – INDICATES FOUND MONUMENT AS NOTED

▲ – CONTINUOUSLY OPERATING REFERENCE STATION (CORS), OPERATED AND MAINTAINED BY THE NATIONAL GEODETIC SURVEY (NGS), DATA AVAILABLE AT HTTPS://WWW.NGS.NOAA.GOV, SEE STATION PID HEREON FOR ADDITIONAL INFORMATION

1 – PID: DH7046 / NGS DESIGNATION: EWPP
NORTH: 1860639.60 EAST: 6705286.96 [GRID]
EPOCH: 2010.00

2 – PID: DH7093 / NGS DESIGNATION: MLFP
NORTH: 1793388.27 EAST: 6768598.36 [GRID]
EPOCH: 2010.00

3 – FOUND 1"IP W/ P.P. "LS 2851" DN. 0.6', NO REFERENCE, ACCEPTED AS ANGLE POINT OF ℄ SAN TIMOTEO CANYON ROAD

4 – FOUND 1"IP (EMPTY) DN. 0.5' IN A.C. PAVEMENT, NO REFERENCE, ACCEPTED AS SW CORNER OF REMAINDER PARCEL AS SHOWN ON R2

5 – FOUND 1"IP & P.P. "LS 2851" DN. 0.4', SE CORNER OF REMAINDER PARCEL PER R2

6 – FOUND 1"IP W/ P.P. "LS 2851" DN. 0.8', SW CORNER OF LOT 10 AS SHOWN ON MB 9/39, PER R3

7 – SNF, ESTABLISHED W'LY CORNER OF R4 AT RECORD DISTANCE (582.20') FROM CN 1/16 CORNER, SEC. 32, PER R4.

8 – FOUND MAG NAIL & WASHER "LS 7232 CROFT" FLUSH IN A.C. PAVEMENT, ACCEPTED AS INTERSECTION OF ℄ TERRACINA BLVD WITH THE N. LINE OF THE S. 1/2, NE 1/4, SECTION 32, PER CORNER RECORD 17–0477

MONUMENT NOTES (CONTINUED)

9 – ℄ INTERSECTION OF NEVADA ST. & SAN TIMOTEO CYN. RD. FOUND 1–1/2"IP & TAG "S.B. CO SRVR" DN. 0.5' IN A.C. PAVEMENT, PER R5, R6, & R7

10 – C 1/4 – SECTION 32 FOUND 2" BRASS CAP "T1S R3W C 1/4 32 SBCO SURV 1977" DN. 0.6' IN A.C. PAVEMENT, PER R6 & R7

11 – CE 1/16 – SECTION 32 FOUND 1"IP & TAG "S.B. COUNTY SURVEYOR", DN. 1.0', PER R6, R10, & CSFB 4018/1419

12 – FOUND 3/4"IP & TACK (TAG MISSING), DN. 0.8', ACCEPTED AS INTERSECTION OF ℄ SAN TIMOTEO CYN. ROAD & S'LY LINE, NE 1/4, SEC. 32, PER R5 & CSFB 4018/1419

13 – FOUND 1"IP & TAG "SBCO SURV" DN. 0.3, PER R5 & CSFB 4018/1419, ACCEPTED AS ANGLE POINT ℄ SAN TIMOTEO CYN. RD.

14 – SNF, ESTABLISHED BY INTERSECTION

15 – FOUND 1"IP (EMPTY), DN. 0.3' & ℄ TIES PER CORNER RECORD 17–0487, ACCEPTED AS E. 1/16 CORNER, SEC. 32/29 PER R6 & R10

16 – SNF, ESTABLISHED BY RECORD ANGLE & DISTANCE PER R4

17 – FOUND 2"IP & TAG "LS 2345", DN. 0.2', ACCEPTED AS S'LY CORNER OF PARCEL 2 OF R9, PER R5 & R8

18 – FOUND 1"IP & TAG "RCE 8591", DN. 0.7', FOR NW CORNER OF PARCEL 1 OF R8, PER R8

19 – SNF, ESTABLISHED SW'LY CORNER OF PARCEL 1 OF R8 BY RECORD DISTANCE FROM THE NW'LY CORNER OF PARCEL 1, PER R8

20 – SNF, ESTABLISHED ANGLE POINT OF PARCEL 'B' OF R1 BY RECORD DISTANCE (16.12') FROM THE SW'LY CORNER OF PARCEL 1 OF R8, PER R1

21 – SNF, ESTABLISHED ANGLE POINT OF PARCEL 'B' OF R1 BY RECORD ANGLE & INTERSECTION WITH THE N'LY LINE OF R11, PER R1

22 – FOUND 1"IP W/ P.P. "LS 5553", DN. 0.1', FOR ANGLE POINT IN W'LY LINE OF R11, PER R10

23 – SNF, ESTABLISHED SE'LY CORNER OF PARCEL 'A' OF R1 BY RECORD ANGLE & INTERSECTION, PER R1

24 – SNF, ESTABLISHED SW'LY CORNER OF PARCEL 2 OF R8 BY RECORD DISTANCE FROM THE SW'LY CORNER OF PARCEL 1 OF R8, PER R8

BASIS OF BEARINGS

THE BEARINGS SHOWN HEREON ARE BASED ON THE GRID BEARING OF N43°16'18"W BETWEEN NGS CORS HORIZONTAL CONTROL STATION MLFP (PID DH7093) AND EWPP (PID DH7046) AS PER RECORDS PUBLISHED BY NGS FOR THE 2010.00 EPOCH

SURVEYOR'S NOTES

C. – CALCULATED
DN. – DOWN
IP – IRON PIPE
M. – MEASURED
P.P. – PLASTIC PLUG
SNF – SEARCHED, NOTHING FOUND

DATUM STATEMENT

COORDINATES SHOWN HEREON ARE BASED ON THE CALIFORNIA COORDINATE SYSTEM (CCS83) ZONE V, 1983 NAD (2010.00 EPOCH)

ALL DISTANCES SHOWN HEREON ARE GROUND DISTANCE, UNLESS OTHERWISE NOTED. TO OBTAIN GRID DISTANCES, MULTIPLY GROUND DISTANCES BY 0.9999526487

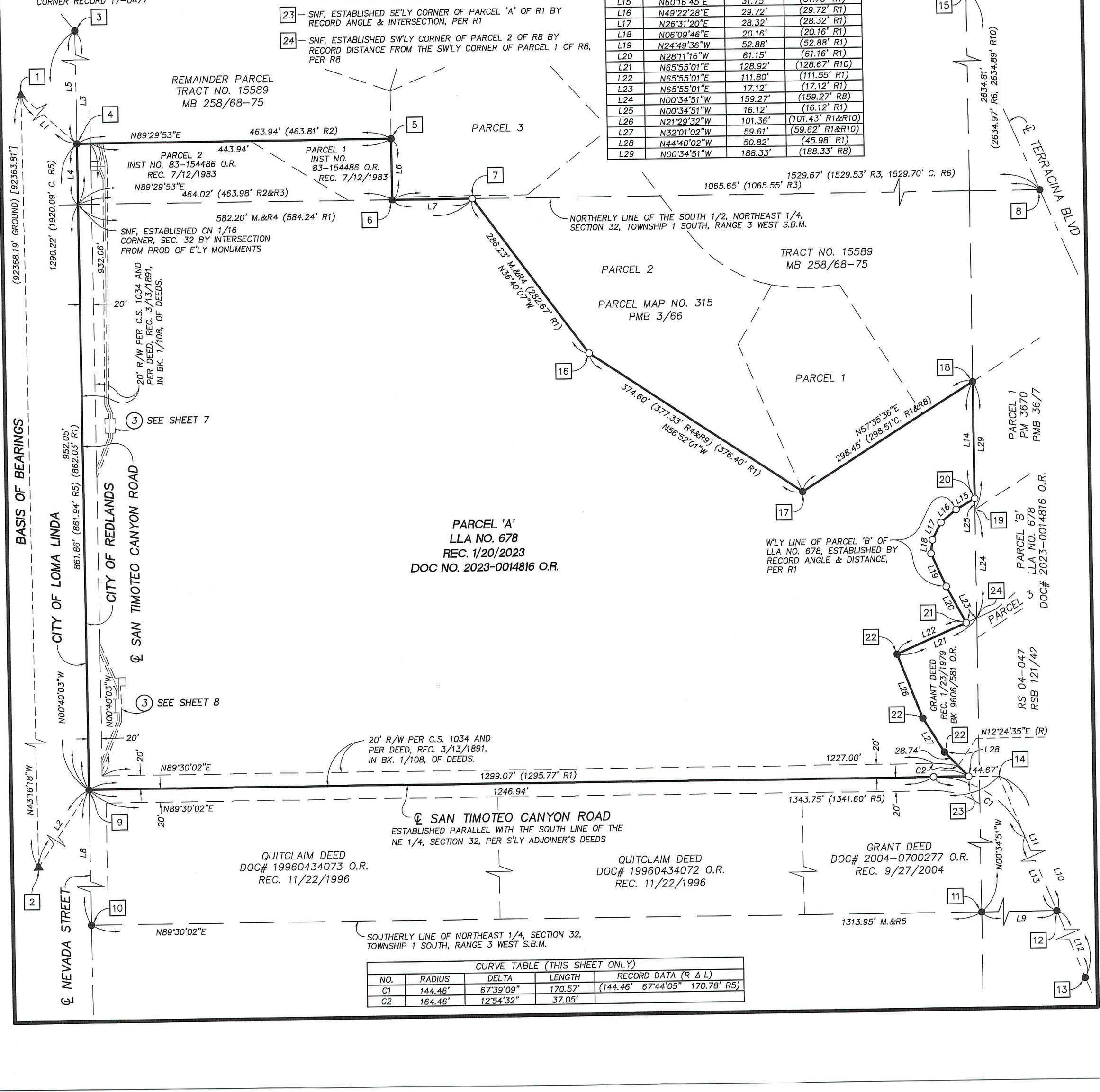
LINE TABLE (THIS SHEET ONLY)

NO.	BEARING	DISTANCE	RECORD DATA	GRID DISTANCE
L1	N77°21'09"W	95805.28' (GROUND)		[95800.74']
L2	N33°39'19"E	54452.69' (GROUND)		[54450.11']
L3	N00°40'03"W	428.36'	(428.15' R5)	
L4	N00°40'03"W	90.19'	(90.23' R2)	
L5	N00°40'03"W	338.17'		
L6	N00°42'57"W	90.19'	(90.23' R2)	
L7	N89°29'53"E	118.18'	(118.25' R9)	
L8	N00°40'20"W	452.63'	(452.68' R5)	
L9	N89°30'07"E	214.51'	(214.54' R5)	
L10	N22°50'49"W	1273.42'	(1277.60' C. R5)	
L11	N22°50'49"W	489.39'	(493.55' R5)	
L12	N22°50'49"W	784.04'	(784.05' R5)	
L13	N22°50'49"W	392.58'		
L14	N00°34'51"W	172.21'	(172.21' R1)	
L15	N60°16'45"E	31.75'	(31.75' R1)	
L16	N49°22'28"E	29.72'	(29.72' R1)	
L17	N26°31'20"E	28.32'	(28.32' R1)	
L18	N06°09'46"E	20.16'	(20.16' R1)	
L19	N24°49'36"W	52.88'	(52.88' R1)	
L20	N28°11'16"W	61.15'	(61.16' R1)	
L21	N65°55'01"E	128.92'	(128.67' R10)	
L22	N65°55'01"E	111.80'	(111.55' R1)	
L23	N65°55'01"E	17.12'	(17.12' R1)	
L24	N00°34'51"W	159.27'	(159.27' R8)	
L25	N00°34'51"W	16.12'	(16.12' R1)	
L26	N21°29'32"W	101.36'	(101.43' R1&R10)	
L27	N32°01'02"W	59.61'	(59.62' R1&R10)	
L28	N44°40'02"W	50.82'	(45.98' R1)	
L29	N00°34'51"W	188.33'	(188.33' R8)	

RECORD REFERENCES

( ) – INDICATES RECORD DATA, AS NOTED
{ } – INDICATES RECORD DATA, PER R1
[ ] – INDICATES GRID DISTANCE
R1 – LLA 678, REC. JANUARY 20, 2023, DOC# 2023–0014816 O.R.
R2 – TRACT NO. 15589, MB 258/68–75
R3 – RECORD OF SURVEY, RSB 104/9–10
R4 – GRANT DEED, REC. MARCH 20, 1952, BK 2917/405 O.R.
R5 – RECORD OF SURVEY, RSB 67/8–10
R6 – RECORD OF SURVEY, RSB 33/95
R7 – COUNTY SURVEYOR'S PLAT C.S.10067
R8 – PARCEL MAP NO. 3670, PMB 36/7
R9 – PARCEL MAP NO. 315, PMB 3/66
R10 – RECORD OF SURVEY 04–047, RSB 121/42
R11 – GRANT DEED, REC. JANUARY 23, 1979, BK 9606/581 O.R.

SCALE: 1"= 100'
0 50' 100' 200'



CURVE TABLE (THIS SHEET ONLY)

NO.	RADIUS	DELTA	LENGTH	RECORD DATA (R Δ L)
C1	144.46'	67°39'09"	170.57'	(144.46' 67°44'05" 170.78' R5)
C2	164.46'	12°54'32"	37.05'	

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

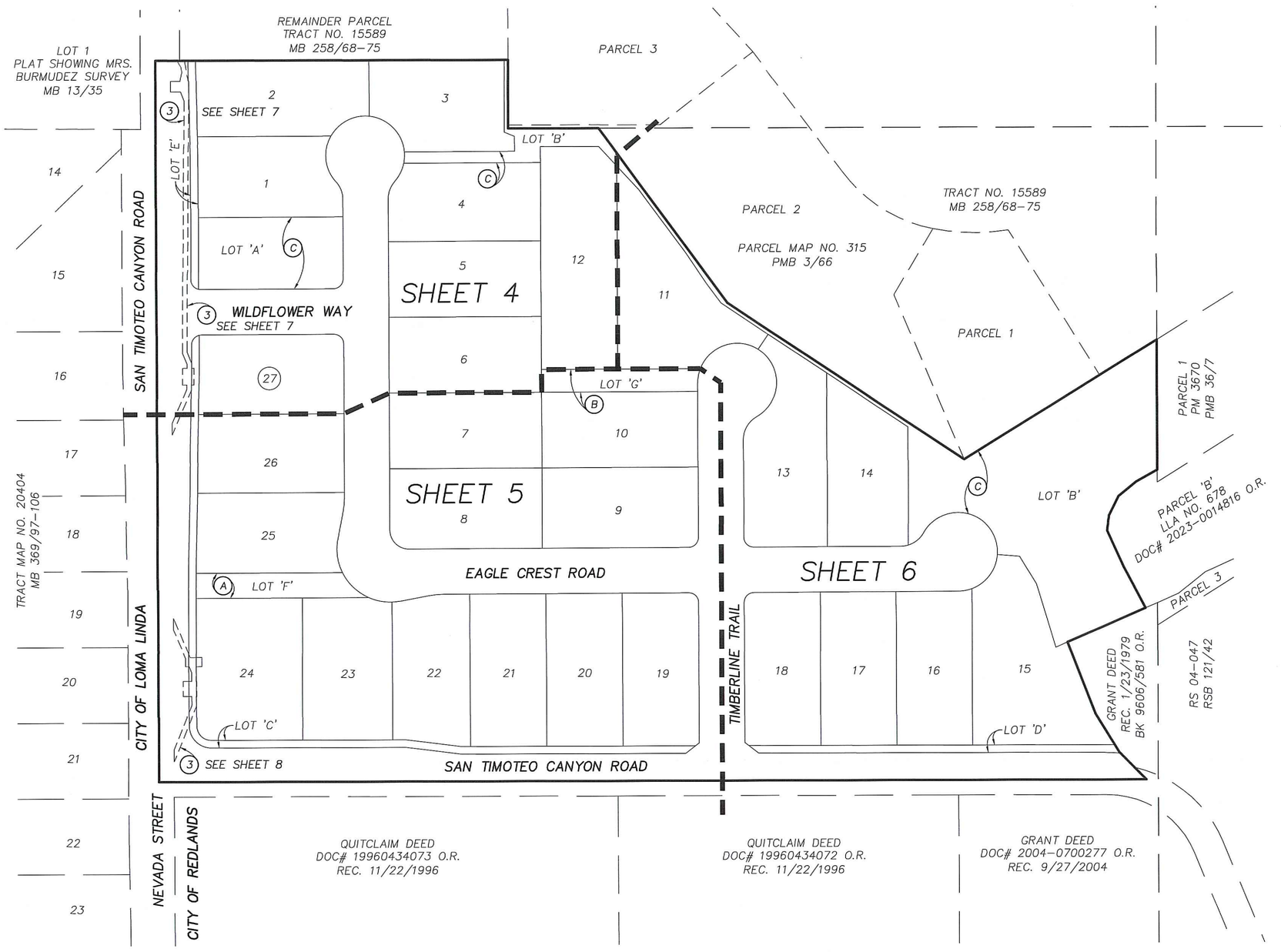
IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106 DATE OF SURVEY: NOVEMBER, 2023

SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES.

INDEX MAP



SCALE: 1"= 100'

0 50' 100' 200'

NOTES

LOT 'A' IS NOT A SEPARATE BUILDING SITE AND IS FOR BASIN PURPOSES.
LOT 'B' IS NOT A SEPARATE BUILDING SITE AND IS FOR OPEN SPACE PURPOSES.
LOTS 'C', 'D' AND 'E' ARE NOT A SEPARATE BUILDING SITES AND ARE FOR LANDSCAPE PURPOSES.
LOT 'F' IS NOT A SEPARATE BUILDING SITE AND IS FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES FOR LOTS 23 AND 24.
LOT 'G' IS NOT A SEPARATE BUILDING SITE AND IS FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES FOR LOTS 11 AND 12.

EXISTING EASEMENTS

1 – EASEMENT FOR PIPE LINES AND INCIDENTAL PURPOSES, GRANTED TO H.H. DANIELS, RECORDED NOVEMBER 20, 1889 IN BOOK 106, PAGE 116 OF DEEDS.
(AMBIGUOUS, NOT LOCATABLE)

2 – EASEMENT FOR PIPE LINES AND INCIDENTAL PURPOSES, GRANTED TO H.H. DANIELS, RECORDED JUNE 12, 1890 IN BOOK 115, PAGE 158 OF DEEDS.
(AMBIGUOUS, NOT LOCATABLE)

(3) – EASEMENT FOR UNDERGROUND ELECTRICAL SUPPLY SYSTEMS, COMMUNICATION SYSTEMS AND INCIDENTAL PURPOSES, GRANTED TO SOUTHERN CALIFORNIA EDISON COMPANY, RECORDED DECEMBER 26, 2025 AS DOCUMENT NO. 2025–0315274 OF OFFICIAL RECORDS.

4 – EASEMENT FOR POLE LINES AND INCIDENTAL PURPOSES, GRANTED TO PACIFIC TELEPHONE AND TELEGRAPH COMPANY, RECORDED DECEMBER 17, 1910 IN BOOK 470, PAGE 3 OF DEEDS.
(AMBIGUOUS, NOT LOCATABLE)

5 – EASEMENT FOR POLE LINES AND INCIDENTAL PURPOSES, GRANTED TO SOUTHERN CALIFORNIA EDISON COMPANY, RECORDED APRIL 2, 1912 IN BOOK 504, PAGE 235 OF DEEDS.
(AMBIGUOUS, NOT LOCATABLE)

EASEMENT NOTES

(A) – EASEMENT OVER ALL OF LOT 'F' FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES FOR THE USE AND BENEFIT OF LOTS 23 AND 24, RESERVED HEREON.

(B) – EASEMENT OVER ALL OF LOT 'G' FOR PRIVATE ACCESS AND PRIVATE UTILITY PURPOSES FOR THE USE AND BENEFIT OF LOTS 11 AND 12, RESERVED HEREON.

(C) – AN EASEMENT OVER ALL OF LOTS 'A' AND 'B' FOR STORM DRAIN PURPOSES, FOR THE USE AND BENEFIT OF THE FUTURE HOMEOWNER'S ASSOCIATION, RESERVED HEREON.

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

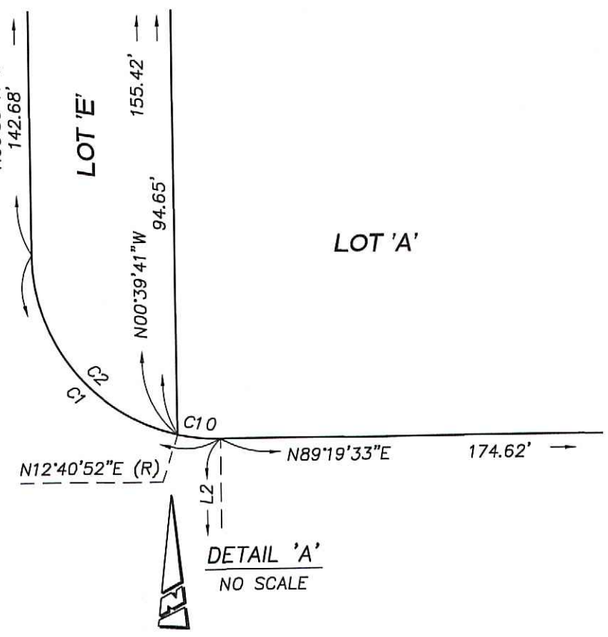
TRACT MAP NO. 20402

IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

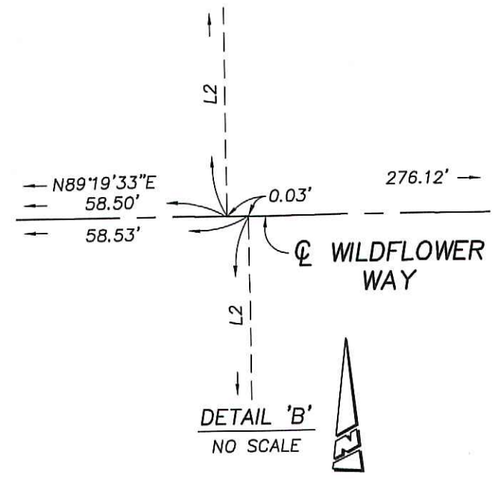
PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106
DATE OF SURVEY: NOVEMBER, 2023

SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES. SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.



LINE TABLE (THIS SHEET ONLY)		
NO.	BEARING	DISTANCE
L1	N89°19'57"E	45.50'
L2	N00°40'27"W	30.00'
L3	N89°19'57"E	45.54'
L4	N00°39'41"W	32.69'
L5	N00°39'41"W	45.35'
L6	N89°19'33"E	30.00'
L7	N68°16'02"W	14.25'
L8	N43°31'29"W	77.41'
L9	N00°29'52"W	19.72'

CURVE TABLE (THIS SHEET ONLY)			
NO.	RADIUS	DELTA	LENGTH
C1	13.00'	90°00'46"	20.42'
C2	13.00'	76°39'27"	17.39'
C3	13.00'	89°59'14"	20.42'
C4	13.00'	76°44'33"	17.41'
C5	13.00'	13°14'41"	3.01'
C6	13.00'	90°00'00"	20.42'
C7	35.00'	41°39'29"	25.45'
C8	52.00'	29°57'24"	27.19'
C9	52.00'	16°36'54"	15.08'
C10	13.00'	13°21'19"	3.03'



SCALE: 1"= 50'

0 25' 50' 100'

REMAINDER PARCEL
TRACT NO. 15589
MB 258/68–75

LOT 1
PLAT SHOWING MRS. BURMUDEZ SURVEY
MB 13/35

PARCEL 3
PARCEL MAP NO. 315
PMB 3/66

PARCEL 2

LOT 'E'
2,983 S.F.
LANDSCAPE PURPOSES

LOT 'A'
18,071 S.F.
BASIN PURPOSES

LOT 'B'
1.71 ACRES
OPEN SPACE

LOT 'C'
11,815 S.F.
LANDSCAPE PURPOSES

LOT 'G'
6,163 S.F.
PRIVATE ACCESS

1 19,137 S.F.
2 21,766 S.F.
3 20,077 S.F.
4 20,249 S.F.
5 20,000 S.F.
6 20,000 S.F.
7
10
11
12 29,108 S.F.
26
27 20,011 S.F.

CITY OF LOMA LINDA
CITY OF REDLANDS
℄ SAN TIMOTEO CANYON ROAD
℄ EAGLE CREST ROAD
℄ WILDFLOWER WAY

TRACT MAP NO. 20404
MB 369/97–106

SEE SHEET 7
SEE SHEET 6
SEE SHEET 5

SEE DETAIL 'A' HEREON
SEE DETAIL 'B' HEREON

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

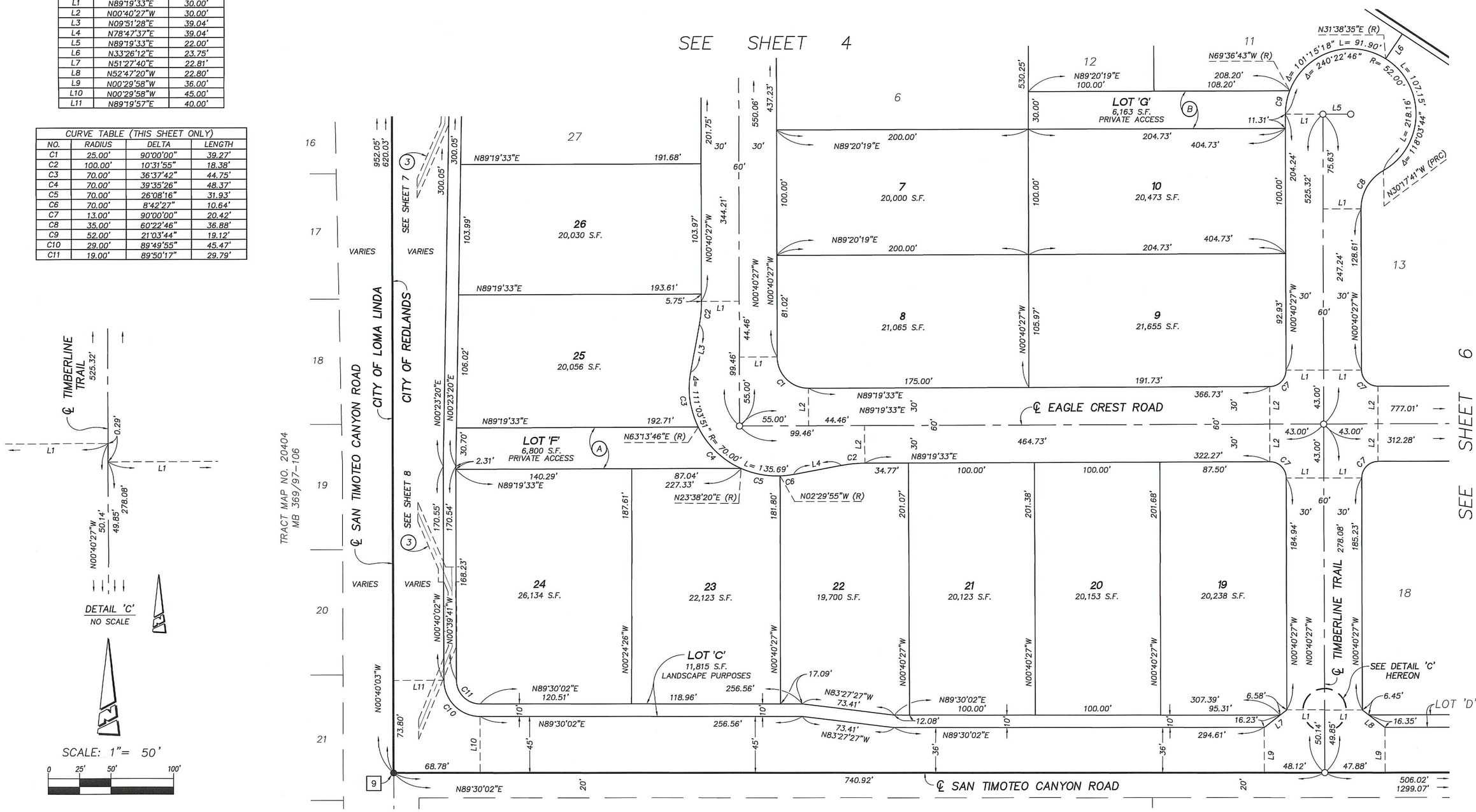
PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106 DATE OF SURVEY: NOVEMBER, 2023

SHEET 5 OF 8 SHEETS

SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES. SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.

LINE TABLE (THIS SHEET ONLY)		
NO.	BEARING	DISTANCE
L1	N89°19'33"E	30.00'
L2	N00°40'27"W	30.00'
L3	N09°51'28"E	39.04'
L4	N78°47'37"E	39.04'
L5	N89°19'33"E	22.00'
L6	N33°26'12"E	23.75'
L7	N51°27'40"E	22.81'
L8	N52°47'20"W	22.80'
L9	N00°29'58"W	36.00'
L10	N00°29'58"W	45.00'
L11	N89°19'57"E	40.00'

CURVE TABLE (THIS SHEET ONLY)			
NO.	RADIUS	DELTA	LENGTH
C1	25.00'	90°00'00"	39.27'
C2	100.00'	10°31'55"	18.38'
C3	70.00'	36°37'42"	44.75'
C4	70.00'	39°35'26"	48.37'
C5	70.00'	26°08'16"	31.93'
C6	70.00'	8°42'27"	10.64'
C7	13.00'	90°00'00"	20.42'
C8	35.00'	60°22'46"	36.88'
C9	52.00'	21°03'44"	19.12'
C10	29.00'	89°49'55"	45.47'
C11	19.00'	89°50'17"	29.79'



NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023–0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83–154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106
DATE OF SURVEY: NOVEMBER, 2023

SHEET 6 OF 8 SHEETS

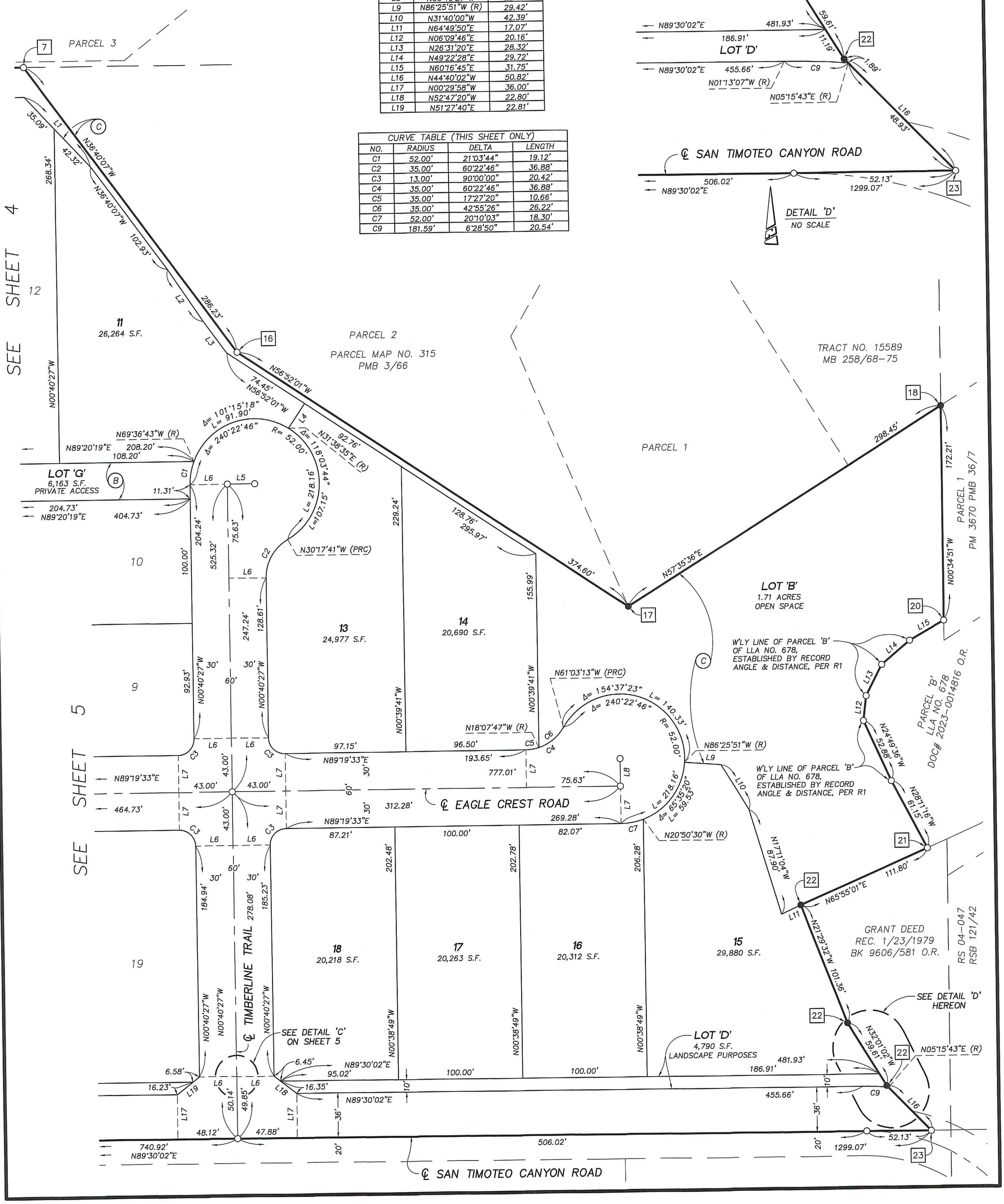
SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES. SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.

SCALE: 1"= 50'

0 25' 50' 100'

LINE TABLE (THIS SHEET ONLY)		
NO.	BEARING	DISTANCE
L1	N43°31'29"W	77.41'
L2	N34°24'59"W	50.90'
L3	N36°40'07"W	31.38'
L4	N33°26'12"E	23.75'
L5	N89°19'33"E	22.00'
L6	N89°19'33"E	30.00'
L7	N00°40'27"W	30.00'
L8	N00°40'27"W	22.00'
L9	N86°25'51"W (R)	29.42'
L10	N31°40'00"W	42.39'
L11	N64°49'50"E	17.07'
L12	N06°09'46"E	20.16'
L13	N26°31'20"E	28.32'
L14	N49°22'28"E	29.72'
L15	N60°16'45"E	31.75'
L16	N44°40'02"W	50.82'
L17	N00°29'58"W	36.00'
L18	N52°47'20"W	22.80'
L19	N51°27'40"E	22.81'

CURVE TABLE (THIS SHEET ONLY)			
NO.	RADIUS	DELTA	LENGTH
C1	52.00'	21°03'44"	19.12'
C2	35.00'	60°22'46"	36.88'
C3	13.00'	90°00'00"	20.42'
C4	35.00'	60°22'46"	36.88'
C5	35.00'	17°27'20"	10.66'
C6	35.00'	42°55'26"	26.22'
C7	52.00'	20°10'03"	18.30'
C9	181.59'	6°28'50"	20.54'



NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

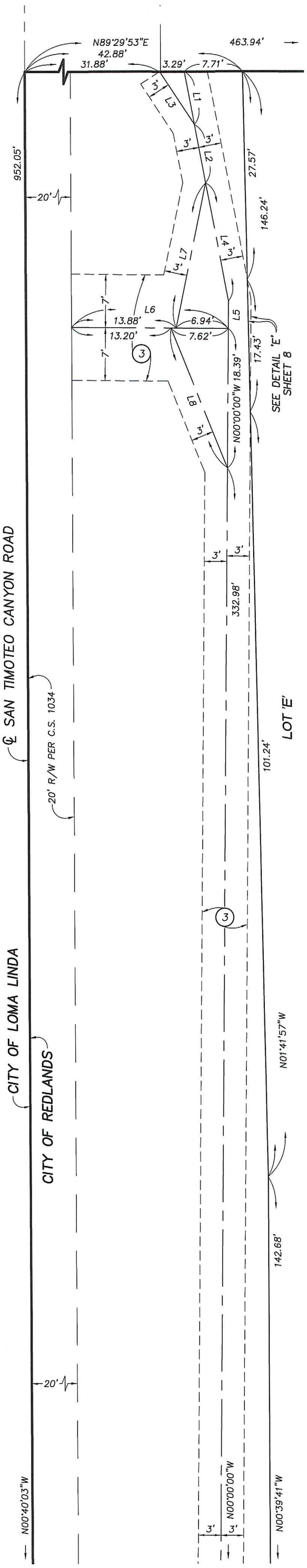
IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

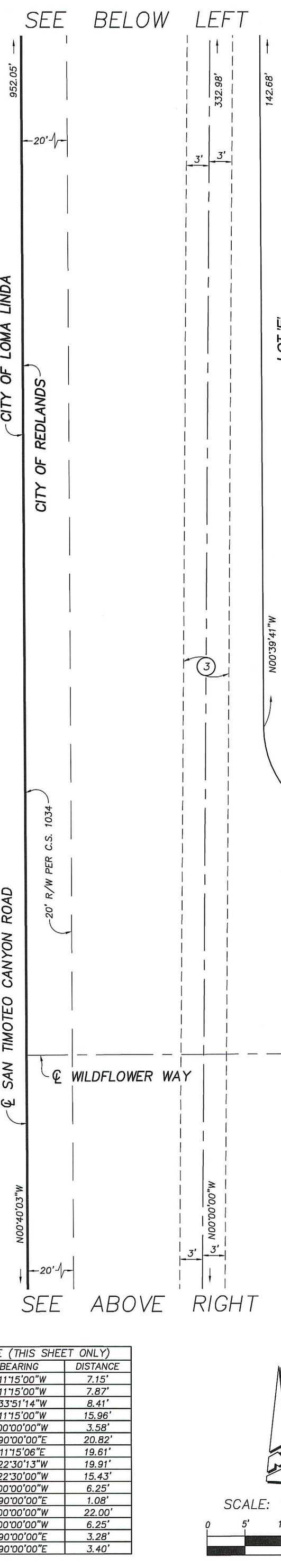
BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023-0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83-154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

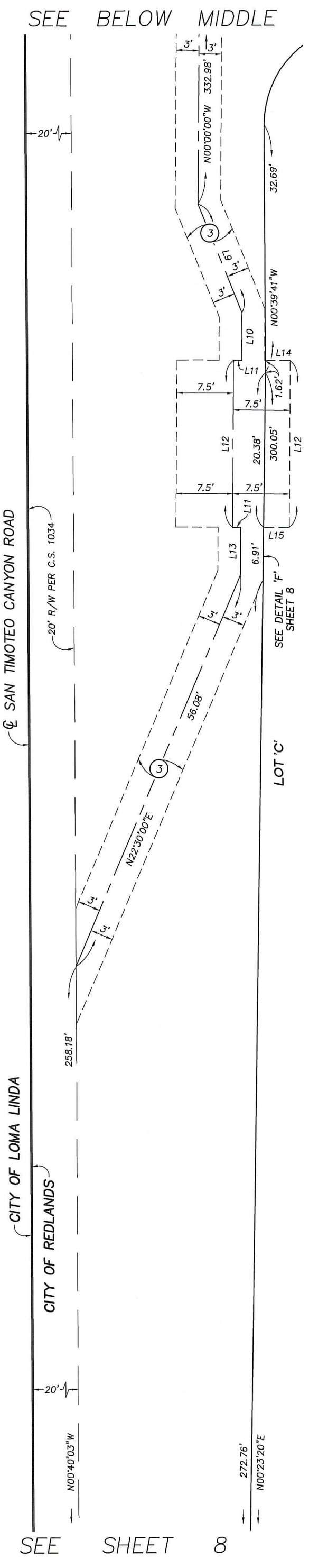
PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106 DATE OF SURVEY: NOVEMBER, 2023

SHEET 7 OF 8 SHEETS

SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES. SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.







LINE TABLE (THIS SHEET ONLY)		
NO.	BEARING	DISTANCE
L1	N11°15'00"W	7.15'
L2	N11°15'00"W	7.87'
L3	N33°51'14"W	8.41'
L4	N11°15'00"W	15.96'
L5	N00°00'00"W	3.58'
L6	N90°00'00"E	20.82'
L7	N11°15'06"E	19.61'
L8	N22°30'13"W	19.91'
L9	N22°30'00"W	15.43'
L10	N00°00'00"W	6.25'
L11	N90°00'00"E	1.08'
L12	N00°00'00"W	22.00'
L13	N00°00'00"W	6.25'
L14	N90°00'00"E	3.28'
L15	N90°00'00"E	3.40'

SCALE: 1"= 10'

0 5' 10' 20'

NUMBERED LOTS: 27
LETTERED LOTS: 7
GROSS ACREAGE: 21.48 ACRES
NET AREA: 16.31 ACRES

TRACT MAP NO. 20402

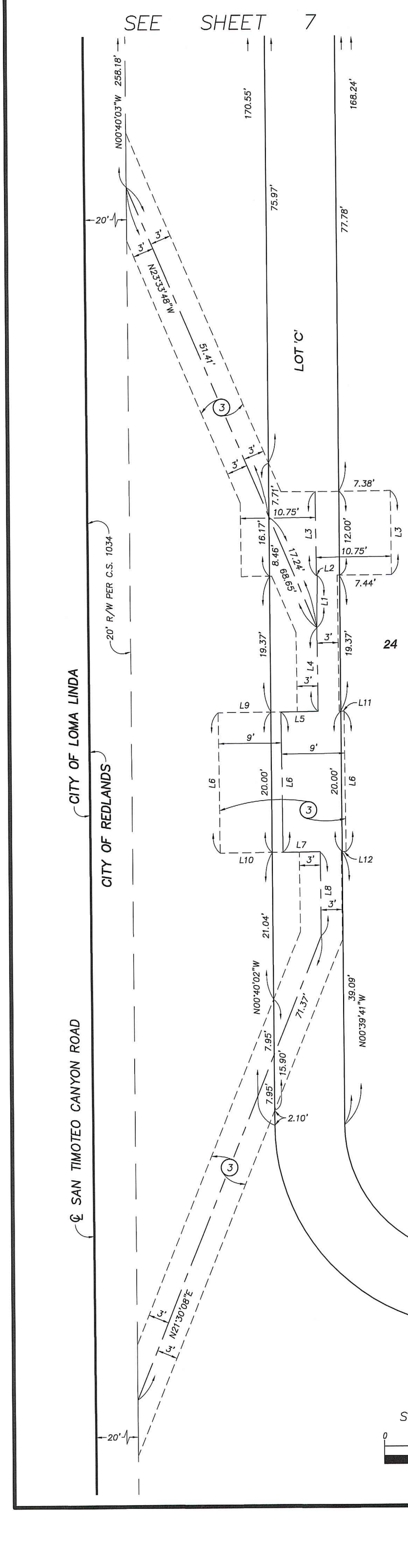
IN THE CITY OF REDLANDS, COUNTY OF SAN BERNARDINO, STATE OF CALIFORNIA

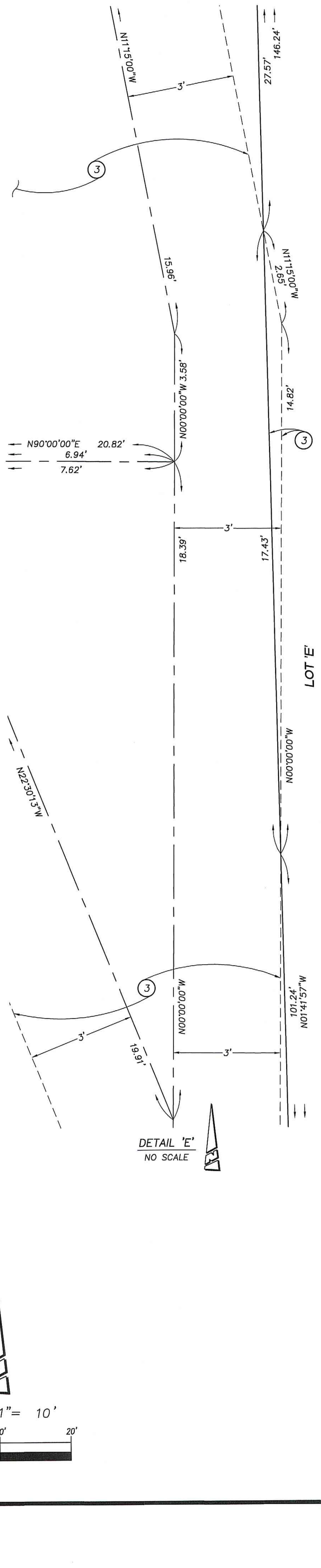
BEING A SUBDIVISION OF PARCEL 'A' OF LOT LINE ADJUSTMENT NO. 678 RECORDED JANUARY 20, 2023 AS DOCUMENT NO. 2023-0014816, TOGETHER WITH PARCELS 1 AND 2 OF THE LAND DESCRIBED IN A GRANT DEED RECORDED JULY 12, 1983 AS INSTRUMENT NO. 83-154486, ALL OF OFFICIAL RECORDS OF SAID COUNTY, LYING WITHIN SECTION 32, TOWNSHIP 1 SOUTH, RANGE 3 WEST, SAN BERNARDINO MERIDIAN

PROACTIVE ENGINEERING CONSULTANTS, INC.
CHARLES J. MOORE, L.S. 9106
DATE OF SURVEY: NOVEMBER, 2023

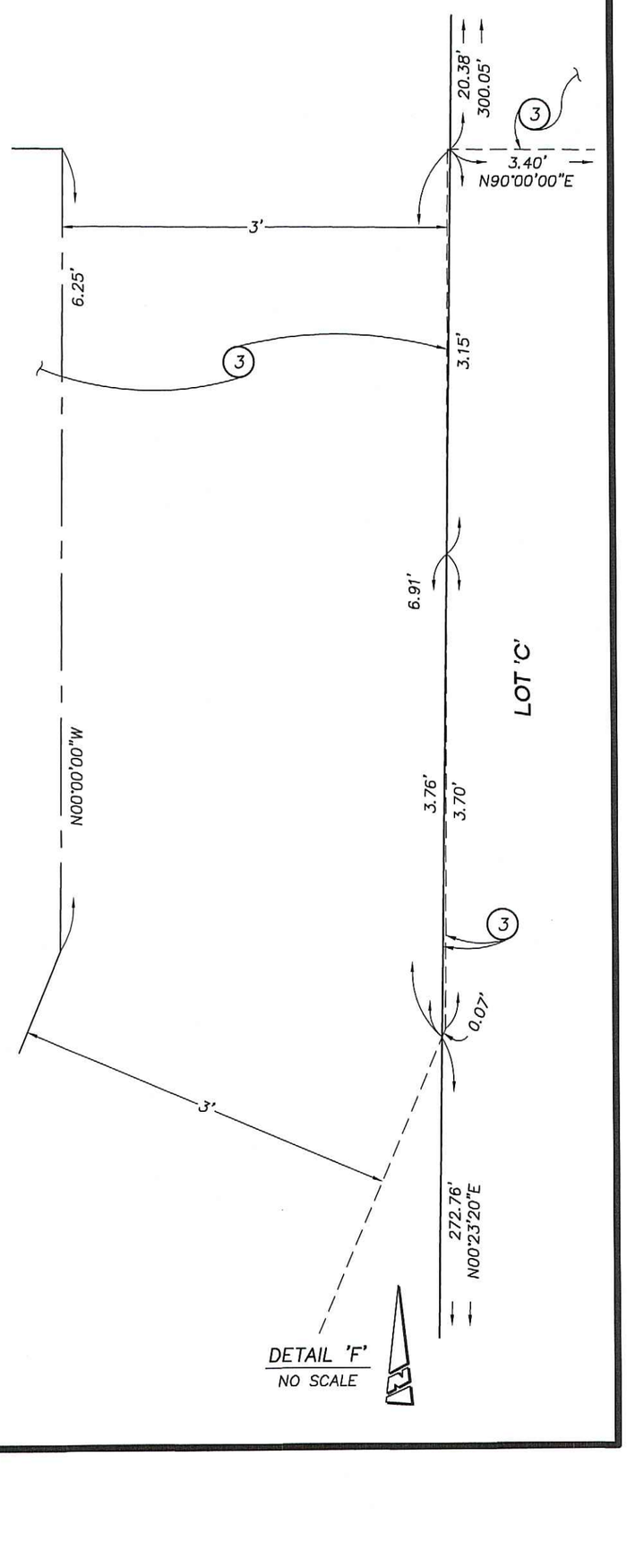
SHEET 8 OF 8 SHEETS

SEE SHEET 2 FOR MONUMENT NOTES, BASIS OF BEARINGS, SURVEYOR'S NOTES, DATUM STATEMENT AND RECORD REFERENCES. SEE SHEET 3 FOR NOTES, EXISTING EASEMENTS AND EASEMENT NOTES.





LINE TABLE (THIS SHEET ONLY)		
NO.	BEARING	DISTANCE
L1	N00°20'39"E	7.46'
L2	N89°02'35"E	0.14'
L3	N00°57'25"W	12.00'
L4	N00°57'25"W	11.91'
L5	N89°02'35"E	5.31'
L6	N00°57'25"W	20.00'
L7	N89°02'35"E	5.31'
L8	N00°57'25"W	12.01'
L9	N89°02'35"E	7.54'
L10	N89°02'35"E	7.44'
L11	N89°02'35"E	0.45'
L12	N89°02'35"E	0.56'



RECORDING REQUESTED BY:
MUNICIPAL UTILITIES AND
ENGINEERING DEPARTMENT
CITY OF REDLANDS

WHEN RECORDED RETURN TO:
CITY CLERK'S OFFICE
CITY OF REDLANDS
P.O. BOX 3005
REDLANDS, CA 92373

(THIS SPACE FOR RECORDER'S USE ONLY)

CITY OF REDLANDS

SUBDIVISION IMPROVEMENT AGREEMENT

This Subdivision Improvement Agreement ("Agreement") is made this 1st day of September, 2026 ("Effective Date"), by and between the City of Redlands, a municipal corporation, hereinafter referred to as "City," and TH Canyon Ranch Loma Linda LLC, a California limited liability company, hereinafter referred to as "Subdivider." City and Subdivider are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

RECITALS

WHEREAS, Subdivider is the owner or authorized developer of property located in the City of Redlands known as Tract No. 20402 (the "Subdivision") for which Subdivider is obligated to construct certain improvements (the "Improvements") as a condition of approval of the Subdivision; and

WHEREAS, City desires to ensure that the Improvements will be constructed in a good and workmanlike manner and in accordance with City laws; and

WHEREAS, Subdivider acknowledges that it is familiar with the provisions of the Redlands Municipal Code and the State Subdivision Map Act (Government Code section 66410 et seq.) and agrees to comply therewith; and

WHEREAS, a final map for the Subdivision has been prepared pursuant to the Redlands Municipal Code and the State Subdivision Map Act, and has been filed by Subdivider for consideration by City;

NOW, THEREFORE, in consideration of the approval and acceptance by the City Council of City of the final map for the Subdivision, and the mutual promises contained herein, the Parties agree as follows:

AGREEMENT

1. Definition and Ownership of Improvements. The Improvements include but are not limited to the grading, paving, construction of curbs and gutters, storm drains and sanitary sewers, water lines, utilities, street lights and all appurtenant facilities associated with the Subdivision that are shown in the plans, profiles and specifications that have been prepared by Subdivider and approved by City, and which are described in Exhibit "A." All Improvements constructed or installed pursuant to this Agreement shall become the property of City, without payment therefor, upon acceptance of those Improvements by City.

2. Time for Completion. Construction of the Improvements shall be completed within twenty-four months from the Effective Date of this Agreement. In the event Subdivider fails to complete construction of the Improvements within that time period, City may require Subdivider's surety to complete the Improvements, or City may complete construction of the Improvements and recoup its expenses for such work from Subdivider, or Subdivider's surety, as hereafter provided.

3. Subdivider's Obligations to Construct Improvements. Subdivider shall:

A. Complete the Improvements, at Subdivider's expense, in conformance with approved Improvement plans; provided, however, that the Improvements shall not be deemed to be completed until accepted by City as provided in Section 18 hereof.

B. Furnish at Subdivider's expense the necessary materials, provisions and other supplies or equipment used for the Improvements, and a payment bond with respect to such work or labor as required by Civil Code Section 9550, for the completion of the Improvements in conformity with the Improvement plans.

C. Acquire and dedicate all rights-of-way, easements, and other interests in real property for construction and installation of the Improvements, or pay the cost of acquisition incurred by City. All rights-of-way, easements and other interests in real property shall be free and clear of liens and encumbrances. Subdivider's obligations with regard to acquisition by City of offsite rights-of-way, easements and other interests in real property shall be subject to a separate agreement between Subdivider and City. Subdivider shall also be responsible for obtaining any public or private sanitary sewer, drainage, and/or utility easements or authorization to accommodate the Subdivision.

D. Commence construction of the Improvements by the time established in Section 25 of this Agreement and complete the Improvements as required by Section 2, above, unless a time extension is granted in writing by City.

E. Install all Improvement monuments required by law prior to acceptance of the Improvements by City. Individual property monuments shall be installed within written number (number) months of such acceptance.

F. Install street name signs conforming to City standards. Permanent street name signs shall be installed before acceptance of the Improvements by City.

4. Acquisition and Dedication of Property. If any of the Improvements contemplated by this Agreement are to be constructed or installed on property not owned by City or Subdivider, no construction or installation shall be commenced before:

A. The offer of dedication to City of appropriate rights-of-way, easements or other interests in real property, and appropriate authorization from property owner to allow construction or installation of the Improvements, or

B. The dedication to, and acceptance by, City of appropriate rights-of-way easements or other interests in real property, as determined by the Municipal Utilities and Engineering Director, or

C. The issuance by a court of competent jurisdiction pursuant to the State Eminent Domain Law of an order of possession. Subdivider shall comply in all respects with the order of possession.

Nothing in this Section shall be construed as authorizing or granting an extension of time to Subdivider.

5. Security. Subdivider shall at all times guarantee Subdivider's performance by furnishing to City and maintaining good and sufficient security as required by the Subdivision laws in accordance with Sections 66499 through 66499.10 of the Government Code, on forms approved by City for the purposes and in the amounts as follows:

A. To assure faithful performance of the Agreement in regard to the Improvements in an amount of one hundred (100%) of the estimated cost of the Improvements; and

B. To secure payment to any contractor, subcontractor, person renting equipment, or furnishing labor and materials for the Improvements, a bond in the amount of fifty (50%) of the estimated cost of the Improvements; and

C. To guarantee or warranty the Improvements for a period of one (1) year following acceptance thereof by City against any defective work or labor done or defective materials furnished in the additional amount of ten (10%) of the estimate cost of the Improvements; and

D. Good and sufficient security in the amount of one hundred (100%) of the estimated cost of setting subdivision monuments.

E. Additional security as required by the applicable provisions of the Redlands Municipal Code.

The securities required by this Agreement shall be kept on file with the City Clerk. The terms of the security documents referenced in this Agreement are hereby incorporated into this Agreement. If any security is replaced by another approved security, the replacement shall: (1) comply with all the requirements for security in this Agreement, (2) be provided to the City Engineer to be filed with the City Clerk, and upon filing (3) be deemed to have been made a part of and incorporated into this Agreement. Upon provision of a replacement security with the City Engineer and

filing of a replacement security with the City Clerk, the former security may be released.

6. Alterations to Improvement Plans.

A. Any changes, alterations or additions to the Improvement plans, not exceeding ten (10%) of the original estimated cost of the Improvements, which are mutually agreed upon by City and Subdivider shall not relieve the Improvement security given for faithful performance of this Agreement. In the event such changes, alterations or additions exceed ten (10%) of the original estimated cost of the Improvements, Subdivider shall provide Improvement security for faithful performance as required by Section 5 of this Agreement for one hundred (100%) of the total estimated cost of the Improvement as changed, altered or amended, less any completed partial releases allowed by Section 8 of this Agreement.

B. Subdivider shall construct the Improvements in accordance with City standards in effect on the Effective Date of this Agreement. City reserves the right to modify the standards applicable to the Subdivision and this Agreement when necessary to protect the public safety or welfare or comply with applicable Federal or State law or City ordinances. If Subdivider requests and is granted an extension of time for completion of the Improvements, City may apply the standards in effect at the time of the extension.

7. Inspection. Subdivider shall at all times maintain proper facilities and safe access for inspection of the Improvements by City inspectors and to the shops wherein any work is in preparation. Upon completion of the Improvements, Subdivider may request a final inspection by the City Engineer or the City Engineer's authorized representative. If the City Engineer, or the City's designated representative, determines that the work has been completed in accordance with this Agreement, then the designated representative shall certify the completion of the Improvements to the Municipal Utilities and Engineering Director/City Engineer. No Improvements shall be accepted unless all aspects of work have been inspected and completed in accordance with the Improvement plans. When applicable law requires an inspection to be made by City at a particular stage of the work of constructing and installing such Improvements, City shall be given timely notice of Subdivider's readiness for such inspection and Subdivider shall not proceed with additional work until the inspection has been made and the work approved. Subdivider shall bear all costs of inspection and certification. No Improvements shall be deemed completed until written acceptance by City.

8. Release of Securities. The securities required by this Agreement shall be released as follows:

A. Security given for faithful performance of any act, obligation, work or agreement shall be released upon the final completion and acceptance of the act or work, subject to the provisions of subsection b. hereof.

B. City may release a portion of the security given for faithful performance of the Improvement work as the work progresses upon application therefor by Subdivider; provided, however, that no such release shall be for an amount less than twenty five (25%) of the total Improvement security given for faithful performance of the Improvement work and that the security shall not be reduced to an amount less than fifty percent (50%) of the total Improvement

security given for faithful performance until final completion and acceptance of the Improvements. In no event shall the City Engineer authorize a release of the Improvement security which would reduce the security to an amount below one hundred twenty five percent (125%) of that required to guarantee completion for the Improvement work and any other obligation imposed by this Agreement.

C. Security given to secure payment to any contractor, subcontractors and to persons furnishing labor, materials or equipment shall, at six (6) months after the completion and acceptance of the work, be reduced to an amount equal to no less than one hundred twenty five percent (125%) of the total claimed by all claimants for whom liens have been filed and of which notice has been given to City, plus an amount reasonably determined by City to be required to assure the performance of any other obligations secured by the security. The balance of the security shall be released upon the settlement of all claims and obligations for which the security was given.

D. No security given for the guarantee or warranty for work shall be released until the expiration of the warranty period and until any claims filed during the warranty period have been settled. As provided in Paragraph 12, the warranty period shall not commence until final acceptance of all the work and Improvements by City.

E. City may retain from any security released, an amount to sufficiently cover costs and reasonable expenses and fees, including reasonable attorneys' fees.

9. Injury to Improvements, Public Property or Public Utilities' Facilities.

A. Subdivider shall replace or repair, or have replaced or repaired, as the case may be, all public Improvements, public utility facilities and surveying or subdivision monuments which are destroyed or damaged as a result of any work under this Agreement. Subdivider shall bear the entire cost of replacement or repairs of any and all public or public utility property damaged or destroyed by reason of any work done under this Agreement, whether such property is owned by the United States or any agency thereof, or the State of California, or any agency or political subdivision thereof, or by City or any public or private utility corporation or by any combination of such owners. Any repair or replacement shall be to the satisfaction, and subject to the approval, of the City Engineer.

B. Furthermore, until such time as the Improvements are accepted by City, Subdivider shall be responsible for, and bear the risk of loss to, the Improvements. Until all Improvements required by this Agreement are fully completed and accepted by City, Subdivider shall be responsible for the care and maintenance of, and any damage to, such Improvements. City shall not, nor shall any officer or employee thereof, be liable to or responsible for any accident, loss or damage, regardless of cause, happening or occurring to the Improvements required by this Agreement prior to the completion and acceptance of the Improvements. All such risks shall be the responsibility of and are hereby assumed by Subdivider.

10. Permits. Subdivider shall, at Subdivider's expense, obtain all necessary permits and licenses for the construction and installation of the Improvements, and give all necessary notices and pay all fees and taxes required by law.

11. Default of Subdivider.

A. Default of Subdivider shall include, but not be limited to:

(1) Subdivider's failure to timely commence construction of the Improvements;
(2) Subdivider's failure to timely complete construction of the Improvements;
(3) Subdivider's failure to timely cure any defect in the Improvements;
(4) Subdivider's failure to perform substantial construction work for a period of twenty (20) calendar days after commencement of the work;
(5) Subdivider's insolvency, appointment of a receiver, or the filing of any petition in bankruptcy, either voluntary or involuntary, which Subdivider fails to discharge within thirty (30) days;
(6) The commencement of a foreclosure action against the subdivision or a portion thereof, or any conveyance in lieu or in avoidance of foreclosure; or
(7) Subdivider's failure to perform any other obligation under this Agreement

B. City reserves to itself all remedies available to it at law or in equity for breach of Subdivider's obligations under this Agreement. City shall have the right, subject to this Section, to draw upon or utilize the appropriate security to mitigate City's damages in the event of default by Subdivider. The right of City to draw upon or utilize the security is additional to and not in lieu of any other remedy available to City. It is specifically recognized that the estimated costs and security amounts may not reflect the actual cost of construction or installation of the Improvements and, therefore, City's damages for Subdivider's default shall be measured by the cost of completing the required Improvements. The sums provided by the Improvements security may be used by City for the completion of the Improvements in accordance with the Improvement plans contained herein.

C. In the event of Subdivider's default under this Agreement, Subdivider authorizes City to perform such obligation twenty (20) days after mailing written notice of default to Subdivider and Subdivider's surety, and agrees to pay the entire cost of such performance by City. City may take over the work and prosecute the same to completion, by contract or by any other method City may deem advisable, for the account and at the expense of Subdivider, and Subdivider's surety shall be liable to City for any excess cost of damages occasioned City thereby. In such event, City, without liability for so doing, may take possession of, and utilize in completing the work, such materials, appliances, plants and other property belonging to Subdivider as may be on the site of the work and necessary for performance of the work.

D. Failure of Subdivider to comply with the terms of this Agreement shall constitute consent to the filing by City of a notice of violation against all the lots in the Subdivision, or to rescind the approval or otherwise revert the Subdivision to acreage. The remedy provided by this subsection is in addition to, and not in lieu of, other remedies available to City. Subdivider agrees that the choice of remedy or remedies for Subdivider's breach shall be in the discretion of City.

E. In the event that Subdivider fails to perform any obligation hereunder, Subdivider agrees to pay all costs and expenses incurred by City in securing performance of such obligations, including but not limited to fees and charges of architects, engineers, attorneys and other professionals, and court costs.

F. The failure of City to take enforcement action with respect to a default, or to declare a breach, shall not be construed as a waiver of that default or breach or any subsequent default or breach of Subdivider.

12. Warranty. Subdivider shall guarantee or warrant the Improvements undertaken pursuant to this Agreement for a period of one (1) year after acceptance of the Subdivision by City against any defective work or labor done or defective materials furnished. If within the warranty period any work or Improvement, or part of any work or Improvement done, furnished, installed or constructed by Subdivider fails to fulfill any of the requirements of this Agreement or the Improvement plans or specifications referred to herein, Subdivider shall without delay and without cost to City repair or replace or reconstruct any defective or otherwise unsatisfactory part or parts of the work or structure. Should Subdivider fail to act promptly in accordance with this requirement, Subdivider hereby authorizes City, at City's option to perform the work twenty (20) days after mailing written notice of default to Subdivider and to Subdivider's surety, and agrees to pay the cost of such work by City. Should City determine that an urgency requires repairs or replacements to be made before Subdivider can be notified, City may, in its sole discretion, make the necessary repairs or replacement or perform the necessary work, and Subdivider shall pay to City the cost of such repairs.

13. Subdivider Not Agent or Employee of City. Neither Subdivider nor Subdivider's agents, contractors or subcontractors are or shall be considered to be agents or employees of City in connection with the performance of Subdivider's obligations under this Agreement.

14. Environmental Warranty. Prior to the acceptance of any property dedications or Improvements by City, Subdivider shall certify and warrant that neither the property to be dedicated nor Subdivider are in violation of any environmental law and neither the property to be dedicated nor the Subdivider are subject to any existing, pending, or threatened investigation by any federal, state or local governmental authority under or in connection with environmental law. Neither Subdivider nor any third party will use, generate, manufacture, produce, or release, on, under, or about the property to be dedicated, any hazardous substance except in compliance with all applicable environmental laws. Subdivider has not caused or permitted the release of, and has no knowledge of the release or presence of, any hazardous substance on the property to be dedicated or the migration of any hazardous substance from or to any other property adjacent to, or in the vicinity of, the property to be dedicated. Subdivider's prior and present use of the property to be dedicated has not resulted in the release of any hazardous substance on the property to be dedicated. Subdivider shall give prompt written notice to City at the address set forth herein of:

A. Any proceeding or investigation by any federal, state or local governmental authority with respect to the presence of any hazardous substance on the property to be dedicated or the migration thereof from or to any other property adjacent to, or in the vicinity of, the property to be dedicated;

B. Any claims made or threatened by any third party against City or the property to be dedicated relating to any loss or injury resulting from any hazardous substance; and

C. Subdivider's discovery of any occurrence or condition on any property adjoining in the vicinity of the property to be dedicated that could cause the property to be dedicated or any

part thereof to be subject to any restrictions on its ownership, occupancy, use for the purpose for which it is intended, transferability or suit under any environmental law.

15. Other Agreements. Nothing contained in this Agreement shall preclude City from expending monies pursuant to agreements concurrently or previously executed between the Parties, or from entering into agreements with other subdividers for the apportionment of costs of the Improvements pursuant to the provisions of the City ordinances providing therefor, nor shall anything in this Agreement commit City to any such apportionment.

16. Subdivider's Obligation to Warn Public during Construction. Until final acceptance of the Improvements by City, Subdivider shall give good and adequate warning to the public of each and every dangerous condition extant in connection with said Improvements, and will take reasonable actions to protect the public from such dangerous conditions.

17. Vesting of Ownership. Upon formal final acceptance of the Improvements by City and recordation of the final map for the Subdivision, ownership of the Improvements constructed pursuant to this Agreement shall vest in City.

18. Final Acceptance of Work. Acceptance of work on behalf of City shall be made by the Municipal Utilities and Engineering Director after final completion and inspection of all Improvements. Such acceptance shall not constitute a waiver of defects by City.

19. Compliance with Laws. Subdivider and its agents, employees, contractors and subcontractors shall comply with all applicable Federal, State and local rules, laws and regulations in constructing the Improvements including, but not limited to, all applicable Labor Code laws.

20. Insurance.

A. City, and its elected and appointed officials, officers, employees, and volunteers shall be covered as additional insureds on the Commercial General Liability ("CGL") policy with respect to liability arising out of work or operations performed by, or on behalf of, Subdivider including materials, parts, or equipment furnished in connection with such work or operations and automobiles owned, leased, hired, or borrowed by or on behalf of Subdivider. General liability coverage can be provided in the form of an endorsement to Subdivider's insurance (at least as broad as Insurance Services Office ("ISO") Form CG 20 10, CG 11 85 or both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 forms if later revisions used).

For any claims related to this project, Subdivider's insurance coverage shall be primary insurance coverage at least as broad as ISO CG 20 01 04 13 as respects City, and its elected and appointed officials, officers, employees, and volunteers. Any insurance or self-insurance maintained by City, and its elected and appointed officials, officers, employees, or volunteers shall be excess of Subdivider's insurance and shall not contribute with it.

Each insurance policy required by this section 20 shall provide that coverage shall not be canceled, except with prior thirty (30) days written notice to City.

B. Builder's Risk (Course of Construction) Insurance. Subdivider may submit evidence of Builder's Risk insurance in the form of Course of Construction coverage. Such

coverage shall name City as a loss payee as their interest may appear.

If the project does not involve new or major reconstruction, at the option of City, an Installation Floater may be acceptable. For such projects, a Property Installation Floater shall be obtained that provides for the improvement, remodel, modification, alteration, conversion or adjustment to existing buildings, structures, processes, machinery and equipment. The Property Installation Floater shall provide property damage coverage for any building, structure, machinery or equipment damaged, impaired, broken, or destroyed during the performance of the Work, including during transit, installation, and testing.

C. Acceptability of Insurers. Insurance is to be placed with insurers authorized to conduct business in the state with a current A.M. Best rating of no less than A: VII, unless otherwise acceptable to City.

D. Waiver of Subrogation. Subdivider hereby agrees to waive rights of subrogation which any insurer of Subdivider may acquire from Subdivider by virtue of the payment of any loss. Subdivider agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation. The Workers' Compensation policy shall be endorsed with a waiver of subrogation in favor of City for all work performed by Subdivider, its employees, agents, and subcontractors.

E. Verification of Coverage. Subdivider shall furnish City with original Certificates of Insurance including all required amendatory endorsements (or copies of the applicable policy language effecting coverage required by this clause) and a copy of the Declarations and Endorsement Page of the CGL policy listing all policy endorsements to City before Work begins. However, failure to obtain the required documents prior to the work beginning shall not waive Subdivider's obligation to provide them. City reserves the right to require complete, certified copies of all required insurance policies, including endorsements, required by these specifications, at any time.

F. Subcontractors. Subdivider shall require and verify that all subcontractors maintain insurance meeting all requirements stated herein, and Subdivider shall ensure that City is an additional insured on insurance required from subcontractors. For CGL coverage, subcontractors shall provide coverage with a form at least as broad as CG 20 38 04 13.

G. Subdivider's Insurance to be Primary

All insurance required by this Agreement is to be maintained by Subdivider for the duration of this Agreement and shall be primary with respect to City and non-contributing to any insurance or self-insurance maintained by City. Subdivider shall provide City with Certificates of Insurance evidencing such insurance concurrent with Subdivider's execution and delivery of this Agreement to City, for City's approval.

H. Worker's Compensation and Employer's Liability. Subdivider shall have Worker's Compensation and Employer's Liability insurance in an amount which meets the statutory requirement with an insurance carrier acceptable to City Subdivider shall execute and provide City with Exhibit "B" titled "Workers' Compensation Insurance Certification," which is attached hereto and incorporated herein by this reference.

I. Comprehensive General Liability Insurance. Subdivider shall secure comprehensive general liability insurance covering all work under this Agreement, including work done by subcontractors, with carriers acceptable to City. Minimum coverage of one million dollars ($1,000,000) per occurrence and two million dollars ($2,000,000) aggregate for public liability, property damage and personal injury is required. City shall be named as an additional insured and the insurance policy shall include a provision prohibiting modification of the coverage limits or cancellation of said policy except upon thirty (30) days prior written notice to City.

J. Business Auto Liability Insurance. Subdivider shall secure business auto liability coverage, with minimum limits of one million dollars ($1,000,000) per occurrence, combined single limit for bodily injury liability and property damage liability. This coverage shall include all Subdivider owned vehicles used on the project, hired and non-owned vehicles, and employee non-ownership vehicles. City shall be named as an additional insured and the insurance policy shall include a provision prohibiting modification of the coverage limits or cancellation of said policy except upon thirty (30) days prior written notice to City.

21. Indemnity/Hold Harmless.

A. City and any official or employee thereof shall not be liable for any injury to persons or property occasioned by reasons of the acts or omissions of Subdivider, its agents, employees, contractors and subcontractors in the performance of this Agreement. Subdivider further agrees to protect, defend, indemnify and hold harmless City, and its officials and employees from any act or omission by Subdivider or its employees or agents, in connection with the work performed pursuant to this Agreement except for all claims, losses, damages, causes of action, injuries and/or liabilities to City and/or third parties caused by the negligence of City or City's agents. This indemnification and Agreement to hold harmless shall extend to injuries to persons and damages or taking of property resulting from the design or construction of the Subdivision, and the public Improvements as provided herein.

B. After acceptance of the Improvements, Subdivider shall remain obligated to eliminate any defect in design or dangerous condition caused by the design or construction defect; however, Subdivider shall not be responsible for routine maintenance. The provisions of this paragraph shall remain in full force and effect for ten (10) years following the acceptance by City of the Improvements. It is the intent of this section that Subdivider shall be responsible for all liability for design and construction of the Improvements installed or work done pursuant to this Agreement and that City shall not be liable for any negligence, nonfeasance, misfeasance or malfeasance in approving, reviewing, checking, or inspecting any work or construction. The Improvement security shall not be required to cover the provisions of this paragraph.

C. Subdivider shall reimburse City for all attorney's fees, costs and expenses (including but not limited to fees and charges of architects, engineers, attorneys and other professionals, and court costs) incurred by City in enforcing the provisions of this section.

D. In the event City tenders defense and indemnification pursuant to the provision set forth in subsection (a) above, and Subdivider wrongfully delays acceptance of the tender of the indemnification beyond the date specified in the tender of defense and indemnification demand,

and based on City's costs necessitated by having to undertake its own defense and utilize the services of its own employees in the defense of any such claim, Subdivider shall be charged two hundred fifty ($250) dollars per day from the date tender should have been accepted until the date tender is finally accepted to reimburse City for all of its defense related expenses, including the value of all time required by City employees to defend City during the time that tender should have been but was not accepted.

22. Personal Nature of Subdivider's Obligations. All of Subdivider's obligations under this Agreement are and shall remain the personal obligations of Subdivider notwithstanding a transfer of all or any part of the property within the Subdivision subject to this Agreement, and Subdivider shall not be entitled to assign its obligations under this Agreement to any transferee of all or any part of the property within the Subdivision or any other third party without the express written consent of City.

23. Sale or Disposition of Subdivision. Subdivider may request a novation of this Agreement and a substitution of security. Upon approval of the novation and substitution of securities, Subdivider may request a release or reduction of the securities required by this Agreement. Nothing in the novation shall relieve Subdivider of the obligations under Section 22 for the work or Improvements done by Subdivider.

24. Time is of the Essence. Time is of the essence in the performance of this Agreement.

25. Time for Commencement of Work; Time Extensions. Subdivider shall commence substantial construction of the Improvements required by this Agreement not later than three (3) months after the Effective Date of this Agreement. In the event good cause exists as determined by the Municipal Utilities and Engineering Director, the time for commencement of construction or completion of the Improvements hereunder may be extended for a period or periods not exceeding a total of two (2) additional years. The extension shall be executed in writing by the Municipal Utilities and Engineering Director. Any such extension may be granted without notice to Subdivider's surety and shall not affect the validity of this Agreement or release the surety or sureties on any security given for this Agreement. The Municipal Utilities and Engineering Director shall be the sole and final judge as to whether or not good cause has been shown to entitle Subdivider to an extension. Delay, other than delay in the commencement of work, resulting from an act of City, act of God, by storm or inclement weather, strikes, boycotts or similar political actions which prevent the conducting of work, which Subdivider could not have reasonably foreseen, and furthermore were not caused by or contributed to by Subdivider, shall constitute good cause for and extension of the time for completion. As a condition of such extension, the Municipal Utilities and Engineering Director may require Subdivider to furnish new security guaranteeing performance of this Agreement, as extended, in an increased amount to compensate for any increase in construction costs as determined by the Municipal Utilities and Engineering Director.

26. Certificate of Satisfaction. The City Manager may, upon the determination of the Development Services Director that Subdivider has fully satisfied the obligations secured by this Agreement, at the request of Subdivider, execute and record a Certificate of Satisfaction in the official records of the County of San Bernardino evidencing Subdivider's compliance with, and satisfaction of, all obligations under this Agreement. Subdivider shall be responsible for the payment of all City costs associated with the preparation and recordation of such a certificate.

27. No Vesting of Rights. Performance by Subdivider of this agreement shall not be construed to vest Subdivider's rights with respect to any change in any zoning or building law or ordinance.

28. Notices. Notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a Party may provide notice in accordance with this section:

Notice to City: Municipal Utilities and Engineering Department
Director City of Redlands
PO Box 3005
Redlands, CA 92373

Notice to Subdivider: TH Canyon Ranch Loma Linda LLC
c/o Trumark Homes LLC
450 Newport Center Drive
Newport Beach, CA 92660
With a copy to:

TH Canyon Ranch Loma Linda LLC
c/o Trumark Properties LLC
3001 Bishop Ranch Drive, Ste 100
San Ramon, CA 94583

ATTN: Legal Department

Such addresses may be changed by notice to the other Party given in the same manner as provided above.

29. Severability. The provisions of this Agreement are severable. If any portion of this Agreement is held invalid by a court of competent jurisdiction, the remainder of the Agreement shall remain in full force and effect unless amended or modified by mutual written consent of the Parties.

30. Captions. The captions of this Agreement are for convenience and reference only and shall not define, explain, modify, limit, exemplify, or aid in the interpretation, construction or meaning of any provisions of this Agreement.

31. Litigation. In the event that suit is brought to enforce the terms of this Agreement, the prevailing party shall be entitled to litigation costs and reasonable attorneys' fees, including

fees for use of in-house counsel by a Party.

32. Incorporation of Recitals. The recitals to this Agreement are hereby incorporated into the terms of this Agreement.

33. Entire Agreement. This Agreement constitutes the entire agreement of the Parties with respect to its subject matter. All modifications, amendments, or waivers of the terms of this Agreement must be in writing and signed by the appropriate representatives of the Parties.

34. Interpretation. This Agreement shall be interpreted in accordance with the laws of the State of California.

35. Jurisdiction. Jurisdiction of all disputes over the terms of this Agreement shall be in the county of San Bernardino, State of California.

IN WITNESS WHEREOF this Agreement is executed by the Parties as of the date herein above first written.

SUBDIVIDER
TH Canyon Ranch Loma Linda LLC, a California limited liability company

By:_____

Guy Oliver,
Vice President of Forward Planning

CITY OF REDLANDS

By:_____

Charles M. Duggan, Jr., City

ATTEST:

_____
Jeanne Donaldson, City Clerk

(Notary attachment and proof of authorization for all signatures required and must be attached)

CALIFORNIA ACKNOWLEDGMENT CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Orange

On September 17th, 2026 before me, Marlise Marae Korzep, Notary Public
Date *Here Insert Name and Title of the Officer*

personally appeared Guy Oliver
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

Place Notary Seal and/or Stamp Above

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature Marlise Marae Korzep
Signature of Notary Public

OPTIONAL

Completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____	Signer's Name: _____
☐ Corporate Officer – Title(s): _____	☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General	☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact	☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator	☐ Trustee ☐ Guardian or Conservator
☐ Other: _____	☐ Other: _____
Signer is Representing: _____	Signer is Representing: _____

©2019 National Notary Association

EXHIBIT "A"

CITY OF REDLANDS
SUBDIVISION IMPROVEMENT AGREEMENT

TRACT MAP NO. 20402

The following plans are in the office of the Municipal Utilities and Engineering Department (MUED);

Description	Drawing No.	No. of Sheets
Street Improvement Plans	2440-ST	09
Storm Drain Improvement Plans	2440-SD	05
Street Striping and Signage Plans (In-Side)	2440-TS1	02
Street Striping and Signage Plans (Out-Side)	2440-TS2	02
Traffic Signal Plans	2440-TS3	01
Street Light Plans	2440-SL	02
Street Tree Plans	2440-TP	05
Force Main Sewer Improvement Plans	F-1876	06
Gravity Sewer Improvement Plans	F-1877	05
Water Improvement Plans	D-60757	08

EXHIBIT "B"

WORKERS' COMPENSATION INSURANCE CERTIFICATION

Every employer, except the State, shall secure the payment of compensation in one or more of the following ways:

(a) By being insured against liability to pay compensation by one or more insurers duly authorized to write compensation insurance in this State.

(b) By securing from the Director of Industrial Relations, a certificate of consent to self-insure, either as an individual employer, or as one employer in a group of employers, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his or her employees.

CHECK ONE

____I am aware of the provisions of Section 3700 of the Labor Code which requires every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code, and I will comply with such provisions before commencing the performance of the work and activities required or permitted under this Agreement. (Labor Code §1861).

____I affirm that at all times, in performing the work and activities required or permitted under this Agreement, I shall not employ any person in any manner such that I become subject to the workers' compensation laws of California. However, at any time, if I employ any person such that I become subject to the workers' compensation laws of California, immediately I shall provide the City with a certificate of consent to self-insure, or a certification of workers' compensation insurance.

I certify under penalty of perjury under the laws of the State of California that the information and representations made in this certificate are true and correct.

TH Canyon Ranch Loma Linda LLC,
a California, LIMITED LIABILITY Company

By:_____ Date: 9-17-26
Guy Oliver, Vice President of Forward Planning

Bond No. PB00224600995
Premium: $48,050.00 / Renews Annually until Released

NOTICE: Bond will not take effect until September 1, 2026

BD-8.2

FAITHFUL PERFORMANCE BOND

Whereas, the City of Redlands ("City"), State of California, and TH Canyon Ranch Loma Linda LCC, a California limited liability company, (hereinafter designated as "Principal") have entered into an agreement dated September 1, 2026 ("Agreement), which is hereby referred to and made a part hereof whereby Principal agrees to install and complete certain designated public improvements (the "Work") for Tract No. 20402; and

Whereas, under the terms of the Agreement, Principal is required before commencing the performance of the Work, to furnish a good and sufficient Faithful Performance bond with the City for the faithful performance of the Agreement;

Now, therefore, we, Principal and the undersigned, as corporate Surety, are held and firmly bound unto the City in the penal sum of Six Million Four Hundred Six Thousand Six Hundred Thirty-Five Dollars ($6,406,635.00) lawful money of the United States, for the payment of which sum we bind ourselves, and our heirs, successors, executors and administrators, jointly and severally, firmly by these presents.

The condition of this obligation is such that if the above bounded Principal, his or its heirs, executors, administrators, successors or assigns, shall in all things stand to and abide by, and well and truly keep and perform the covenants, conditions and provisions in the Agreement and any alteration thereof made as therein provided, on his or its part, to be kept and performed at the time and in the manner therein specified, and in all respects according to their true intent and meaning, and shall faithfully fulfill the one-year guarantee of all materials and workmanship, and shall defend, indemnify and save harmless the City and its elected officials, officers, agents and employees, as therein stipulated, then this obligation shall become null and void; otherwise it shall be and remain in full force and effect.

As a part of the obligation secured hereby and in addition to the face amount specified therefor, there shall be included costs and reasonable expenses and fees, including reasonable attorneys' fees, incurred by the City in successfully enforcing such obligations, all to be taxed as costs and included in the judgment rendered.

As a condition precedent to the satisfactory completion of the Agreement, the above obligation shall hold good for a period of one (1) year or longer if required by the Agreement after the acceptance of the Work by the City, during which time if Principal shall fail to make full, complete, and satisfactory repair and replacements and totally protect the City from loss or damage made evident during this period from the date of completion of the Work, and resulting from or caused by defective materials or faulty workmanship, the above obligation in penal sum thereof shall remain in full force and effect. The obligations of Surety hereunder shall continue so long as any obligation of Principal remains.

Whenever Principal shall be, and is declared by the City to be, in default under the Agreement, the City having performed the City obligations thereunder, the Surety shall promptly

remedy the default, or shall promptly, at the City's option:

1. Complete the Agreement in accordance with its terms and conditions; or

2. Obtain a bid or bids for completing the Agreement in accordance with its terms and conditions, and upon determination by Surety of the lowest responsive and responsible bidder, arrange for a contract between such bidder and the City, and make available as work progresses sufficient funds to pay the cost of completion of the Work less the balance of the Agreement price, but not exceeding, including other costs and damages for which Surety may be liable hereunder, the amount set forth above. The term "balance of the Agreement price," as used in this paragraph, shall mean the total amount payable to Principal by the City under the Agreement and any modifications thereto, less the amount previously properly paid by the City to Principal.

Surety expressly agrees that the City may reject any contractor or subcontractor which may be proposed by Surety in fulfillment of its obligations in the event of default by Principal.

Surety shall not utilize Principal in completing the Work nor shall Surety accept a bid from Principal for completion of the Work if the City, when declaring Principal in default, notifies Surety of the City's objection to Principal's further participation in the completion of the Work.

No right of action shall accrue on the bond to or for the use of any person or corporation other than the City named herein or the successors or assigns of the City. Any suit under this bond must be instituted within the applicable statute of limitations period.

Surety, for value received, hereby stipulates and agrees that no change, extension of time, alteration or addition to the terms of the Agreement or to the Work to be performed thereunder or the specifications accompanying the same shall in any way affect its obligations on this bond, and it does hereby waive notice of any such change, extension of time, alteration or addition to the terms of the Agreement or to the Work or to the specifications.

No final settlement between the City and Principal shall abridge the right of any beneficiary hereunder whose claim may be unsatisfied.

Principal and Surety agree that if the City is required to engage the services of any attorney in connection with the enforcement of this bond, each shall pay the City's reasonable attorneys' fees incurred, with or without suit, in addition to the above sum.

In witness whereof, this instrument has been duly executed by Principal and Surety above named, on July 15, 2026.

(SEAL)
TH Canyon Ranch Loma Linda LLC,
a California limited liability company
(Principal)

(Signature) Guy Oliver, Vice President of Forward Planning

(SEAL)
Philadelphia Indemnity Insurance Company
(Surety)

BY:
(Signature) Jan Rivera, Attorney-in-Fact

Address: 283 S. Lake Ave, Suite 160
Pasadena, CA 91101
Telephone (626) 639-1325

(Seal and Notarial Acknowledgment of Surety)

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT **CIVIL CODE § 1189**

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California)
County of Orange)

On 07-15-2026 before me, Lisa Marie Saumur, Notary Public,
Date *Here Insert Name and Title of the Officer*

personally appeared Jan Rivera
Name(s) of Signer(s)

,

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

LISA MARIE SAUMUR
Notary Public - California
Orange County
Commission # 2487918
My Comm. Expires May 3, 2028

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature _____
Signature of Notary Public

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____
Document Date: _____ Number of Pages: _____
Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer Is Representing: _____

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer Is Representing: _____

©2015 National Notary Association • www.NationalNotary.org • 1-800-US NOTARY (1-800-876-6827) Item #5907

PHILADELPHIA INDEMNITY INSURANCE COMPANY
One Bala Plaza, Suite 100
Bala Cynwyd, PA 19004-0950

Power of Attorney

KNOW ALL PERSONS BY THESE PRESENTS: That **PHILADELPHIA INDEMNITY INSURANCE COMPANY** (the Company), a corporation organized and existing under the laws of the Commonwealth of Pennsylvania, does hereby constitute and appoint **Lourdes Landa, Mark Rosskopf, Lisa Saumur, Jan Rivera and Jessica Garcia of McGriff Insurance Services, Inc**its true and lawful Attorney-in-fact with full authority to execute on its behalf bonds, undertakings, recognizances, consents of surety and other contracts of indemnity and writings obligatory in the nature thereof, issued in the course of its business and to bind the Company thereby, in an amount not to exceed **$50,000,000**.

This Power of Attorney is granted and is signed and sealed by facsimile under and by the authority of the following Resolution adopted by the Board of Directors of PHILADELPHIA INDEMNITY INSURANCE COMPANY on the 14th of November 2016.

RESOLVED: That the Board of Directors hereby authorizes the President or any Vice President of the Company: (1) Appoint Attorney(s) in Fact and authorize the Attorney(s) in Fact to execute on behalf of the Company bonds and undertakings, contracts of indemnity and other writings obligatory in the nature thereof and to attach the seal of the Company thereto; and (2) to remove, at any time, any such Attorney-in-Fact and revoke the authority given. And, be it

FURTHER RESOLVED: That the signatures of such officers and the seal of the Company may be affixed to any such Power of Attorney or certificate relating thereto by facsimile, and any such Power of Attorney so executed and certified by facsimile signatures and facsimile seal shall be valid and binding upon the Company in the future with respect to any bond or undertaking to which it is attached.

IN TESTIMONY WHEREOF, PHILADELPHIA INDEMNITY INSURANCE COMPANY HAS CAUSED THIS INSTRUMENT TO BE SIGNED AND ITS CORPORATE SEAL TO BE AFFIXED BY ITS AUTHORIZED OFFICE THIS 21ST DAY OF AUGUST 2025.

(Seal)

John Glomb, President & CEO

Philadelphia Indemnity Insurance Company

On this 21st day of August, 2025, before me came the individual who executed the preceding instrument, to me personally known, and being by me duly sworn said that he is the therein described and authorized officer of the **PHILADELPHIA INDEMNITY INSURANCE COMPANY**; that the seal affixed to said instrument is the Corporate seal of said Company; that the said Corporate Seal and his signature were duly affixed.

Notary Public:

Commonwealth of Pennsylvania - Notary Seal
PAULA LARE - Notary Public
Montgomery County
My Commission Expires October 15, 2026
Commission Number 1193866

residing at: Bala Cynwyd

My commission expires: October 15, 2026

I, Angelique Cooper, Corporate Secretary of PHILADELPHIA INDEMNITY INSURANCE COMPANY, do hereby certify that the foregoing resolution of the Board of Directors and the Power of Attorney issued pursuant thereto on the 21st day of August, 2025 are true and correct and are still in full force and effect. I do further certify that John Glomb, who executed the Power of Attorney as President, was on the date of execution of the attached Power of Attorney the duly elected President of PHILADELPHIA INDEMNITY INSURANCE COMPANY.

In Testimony Whereof I have subscribed my name and affixed the facsimile seal of each Company this 15 day of JULY, 2026.

Angelique Cooper, Corporate Secretary
PHILADELPHIA INDEMNITY INSURANCE COMPANY

CALIFORNIA ACKNOWLEDGMENT CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Orange }

On July 16th, 2020 before me, Marlise Marae Korzep, Notary Public.
Date *Here Insert Name and Title of the Officer*

personally appeared Guy Oliver
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

Place Notary Seal and/or Stamp Above

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature Marlise Marae Korzep
Signature of Notary Public

OPTIONAL

Completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer is Representing: _____

Signer's Name: _____
☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer is Representing: _____

©2019 National Notary Association

Bond No. PB00224600995
Premium: Included

NOTICE: Bond will not take effect until September 1, 2026
BD-8.1

LABOR AND MATERIAL BOND

Whereas, the City Council of the City of Redlands ("City"), State of California, and TH Canyon Ranch Loma Linda LCC, a California limited liability company, (hereinafter as "Principal") have entered into an agreement dated September 1, 2026 ("Agreement"), which is hereby referred to and made a part hereof whereby Principal agrees to install and complete certain designated public improvements ("Work") for Tract Map No. 20402; and

Whereas, under the terms of the Agreement, Principal is required, before commencing the performance of the Work, to file a good and sufficient Labor and Material bond with the City to secure the claims to which reference is made in Title 3 (commencing with Section 9550) of Part 6 of Division 4 of the Civil Code of the State of California;

Now, therefore, Principal and the undersigned, as Surety, are held firmly bound unto the City and all contractors, subcontractors, laborers, material men, and other persons employed in the performance of the Agreement and referred to in the aforesaid Civil Code the sum of Three Million Two Hundred Three Thousand Three Hundred Seventeen and 50/100ths Dollars ($3,203,317.50) for materials furnished or labor thereon of any kind, or for amounts due under the Unemployment Insurance Act with respect to the Work or labor, that said Surety will pay the same in an amount not exceeding the amount hereinabove set forth, and also in case suit is brought upon this bond, will pay, in addition to the face amount thereof, costs and reasonable expenses and fees, including reasonable attorneys' fees, incurred by the City in successfully enforcing such obligation, to be awarded and fixed by the court, and to be taxed as costs and to be included in the judgment therein rendered.

It is hereby expressly stipulated and agreed that this bond shall inure to the benefit of any and all persons, companies and corporations entitled to file claims under Title 3 (commencing with Section 9550) of Part 6 of Division 4 of the Civil Code, so as to give a right of action to them or their assigns in any suit brought upon this bond. Should the condition of this bond be fully performed, then this obligation shall become null and void, otherwise it shall be and remain in full force and effect.

The Surety hereby stipulates and agrees that no change, extension of time, alteration or addition to the terms of the Agreement or the specifications accompanying the same shall in any manner affect its obligations on this bond, and it does hereby waive notice of any such change, extension of time, alteration or addition.

In witness whereof, this instrument has been duly executed by Principal and Surety above named, on July 15, 2026.

(SEAL)
TH Canyon Ranch Loma Linda LLC,
a California limited liability company
(Principal)

(Signature) Guy Oliver, Vice President of Forward Planning

(SEAL)

Philadelphia Indemnity Insurance Company
(Surety)
BY:

(Signature) Jan Rivera, Attorney-in-Fact

Address:
283 S. Lake Ave, Suite 160
Pasadena, CA 91101

Telephone(626) 639-1325

(Seal and Notarial Acknowledgment of Surety)

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT **CIVIL CODE § 1189**

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California)
County of Orange)

On 07-15-2026 before me, Lisa Marie Saumur, Notary Public,
Date *Here Insert Name and Title of the Officer*

personally appeared Jan Rivera
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

LISA MARIE SAUMUR
Notary Public · California
Orange County
Commission # 2487918
My Comm. Expires May 3, 2028

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature
Signature of Notary Public

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____
Document Date: _____ Number of Pages: _____
Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer Is Representing: _____

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer Is Representing: _____

©2015 National Notary Association • www.NationalNotary.org • 1-800-US NOTARY (1-800-876-6827) Item #5907

PHILADELPHIA INDEMNITY INSURANCE COMPANY
One Bala Plaza, Suite 100
Bala Cynwyd, PA 19004-0950

Power of Attorney

KNOW ALL PERSONS BY THESE PRESENTS: That **PHILADELPHIA INDEMNITY INSURANCE COMPANY** (the Company), a corporation organized and existing under the laws of the Commonwealth of Pennsylvania, does hereby constitute and appoint **Lourdes Landa, Mark Rosskopf, Lisa Saumur, Jan Rivera and Jessica Garcia of McGriff Insurance Services, Inc**its true and lawful Attorney-in-fact with full authority to execute on its behalf bonds, undertakings, recognizances, consents of surety and other contracts of indemnity and writings obligatory in the nature thereof, issued in the course of its business and to bind the Company thereby, in an amount not to exceed **$50,000,000.**

This Power of Attorney is granted and is signed and sealed by facsimile under and by the authority of the following Resolution adopted by the Board of Directors of PHILADELPHIA INDEMNITY INSURANCE COMPANY on the 14th of November 2016.

RESOLVED: That the Board of Directors hereby authorizes the President or any Vice President of the Company: (1) Appoint Attorney(s) in Fact and authorize the Attorney(s) in Fact to execute on behalf of the Company bonds and undertakings, contracts of indemnity and other writings obligatory in the nature thereof and to attach the seal of the Company thereto; and (2) to remove, at any time, any such Attorney-in-Fact and revoke the authority given. And, be it

FURTHER RESOLVED: That the signatures of such officers and the seal of the Company may be affixed to any such Power of Attorney or certificate relating thereto by facsimile, and any such Power of Attorney so executed and certified by facsimile signatures and facsimile seal shall be valid and binding upon the Company in the future with respect to any bond or undertaking to which it is attached.

IN TESTIMONY WHEREOF, PHILADELPHIA INDEMNITY INSURANCE COMPANY HAS CAUSED THIS INSTRUMENT TO BE SIGNED AND ITS CORPORATE SEAL TO BE AFFIXED BY ITS AUTHORIZED OFFICE THIS 21ST DAY OF AUGUST 2025.

(Seal)

John Glomb, President & CEO

Philadelphia Indemnity Insurance Company

On this 21st day of August, 2025, before me came the individual who executed the preceding instrument, to me personally known, and being by me duly sworn said that he is the therein described and authorized officer of the **PHILADELPHIA INDEMNITY INSURANCE COMPANY**; that the seal affixed to said instrument is the Corporate seal of said Company; that the said Corporate Seal and his signature were duly affixed.

Notary Public:

Commonwealth of Pennsylvania - Notary Seal
PAULA LARE - Notary Public
Montgomery County
My Commission Expires October 15, 2026
Commission Number 1193866

residing at: Bala Cynwyd

My commission expires: October 15, 2026

I, Angelique Cooper, Corporate Secretary of PHILADELPHIA INDEMNITY INSURANCE COMPANY, do hereby certify that the foregoing resolution of the Board of Directors and the Power of Attorney issued pursuant thereto on the 21st day of August, 2025 are true and correct and are still in full force and effect. I do further certify that John Glomb, who executed the Power of Attorney as President, was on the date of execution of the attached Power of Attorney the duly elected President of PHILADELPHIA INDEMNITY INSURANCE COMPANY.

In Testimony Whereof I have subscribed my name and affixed the facsimile seal of each Company this 15 day of JULY, 2026.

Angelique Cooper, Corporate Secretary
PHILADELPHIA INDEMNITY INSURANCE COMPANY

CALIFORNIA ACKNOWLEDGMENT CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Orange }

On July 16th, 2026 before me, Marlise Marae Korzep, Notary Public,
Date *Here Insert Name and Title of the Officer*

personally appeared Guy Oliver
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

MARLISE MARAE KORZEP
Notary Public - California
Orange County
Commission # 2550122
My Comm. Expires Mar 17, 2030

Place Notary Seal and/or Stamp Above

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature Marlise Marae Korzep
Signature of Notary Public

OPTIONAL

Completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer is Representing: _____

Signer's Name: _____
☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
Signer is Representing: _____

©2019 National Notary Association

City Council **AGENDA ITEM NO. I9.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve an Agreement with TH Canyon Ranch Loma Linda, LLC regarding operation and maintenance of a private lift station and force main serving Tract No. 20402 in San Timoteo Canyon and determine that the approval of the proposed agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's guidelines implementing the California Environmental Quality Act (Development Services Director Reilly)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that the approval of the proposed agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act; and

2. I move that the City Council approve the agreement with TH Canyon Ranch Loma Linda LLC for the operation and maintenance of a private lift station and force main serving Tract No. 20402 in San Timoteo Canyon.

RECOMMENDATION:

Staff recommends that the City Council approve the agreement with TH Canyon Ranch Loma Linda, LLC for operation and maintenance of a private lift station and force main serving Tract No. 20402 in San Timoteo Canyon and determine that the approval of the proposed agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act.

DISCUSSION:

On December 12, 2023, the Planning Commission approved Tentative Tract Map No. 20402 through Resolution No. 1656, authorizing a residential subdivision consisting of 27 single-family lots and associated infrastructure. Resolution No. 1656 anticipated the construction of utility improvements, including sewer facilities, subject to subsequent engineering review and approval by the City prior to recordation and construction.

While Resolution No. 1656 did not approve detailed sewer design, it expressly required that all utilities be reviewed and approved through later-stage permits, including improvement plans and utility agreements, in accordance with City standards.

The location of the development approximately one half mile south of Barton Road along San Timoteo Canyon Road (see Attachment B) cannot reasonably be served by a gravity sewer main. A gravity sewer main would require the pipe to be over 25 feet deep in some locations, which would be a logistical problem for future maintenance and operations. Instead of a gravity sewer main, the developer intends to install a privately operated sewer lift station at the western boundary of the tract, which will then pump effluent through a private sewer force main to the existing City owned sewer main at the intersection of Barton Road and Nevada Street. The developer has coordinated with the City of Loma Linda to establish an emergency overflow connection to the Loma Linda sewer system for use only if the proposed sewer lift station experiences problems or failure.

The applicant has submitted a Private Sewer Lift Station and Force Main Engineering Design Report and Emergency Response Plan, prepared by Proactive Engineering Consultants and peer-reviewed**,** dated November 26, 2025. The Emergency Response Plan was reviewed by the Sewer Division of the Municipal Utilities and Engineering Department and deemed appropriate.

The proposed improvements related to the agreement include:

- An 8-inch public gravity sewer conveying wastewater to a private lift station.
- A private sewer lift station located near San Timoteo Canyon Road and Wildflower Way.
- A 4-inch private sewer force main, constructed of C900 DR14 PVC, conveying wastewater north to an existing 18-inch public gravity sewer at Barton Road and Nevada Street.
- A private emergency overflow connection allowing temporary gravity flow in the event of lift station failure, subject to approval by the City of Loma Linda.
- Remote monitoring, emergency storage capacity, odor mitigation, and a detailed emergency response protocol.

The sewer lift station, sewer force main and overflow facilities are designed to serve Tract No. 20402 and will remain private, with long-term maintenance responsibility assigned to the homeowners association for the tract.

The developer requests that the City enter into an agreement for the private lift station and sewer force main whereby the developer will be responsible for the operation and maintenance of the facilities (see Attachment A). If the City of Redlands incurs costs resulting from the operation of the sewer system for this tract, those costs are to be reimbursed by the developer or the homeowners association, who will ultimately become the responsible party per the terms of the agreement.

The developer will enter into an agreement with the City of Loma Linda regarding any event necessitating the use of the emergency overflow.

ALTERNATIVES:

The City Council may choose not to approve the agreement. However, doing so will adversely affect the developer’s plans for the housing project and may present a potential liability to the City as the proposed sewer improvements are included within the scope of the approved project.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Sean Reilly, Development Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager

James Garland, Finance Director
Monica Heredia, Municipal Utilities and Engineering Director

PREPARED BY:
Don Young, One Stop Permit Center Manager

FISCAL IMPACT

Fiscal Year:

Revenue Generating: No

Amount: $

Budgeted Y/N: N/A

Account No.:

Additional Appropriation Required: No

Discussion:

There is no fiscal impact to the City's General Fund or Sewer Fund. All costs associated with the design, construction, operation, and maintenance of the private sewer facilities will be borne by the developer and, upon formation, the homeowners association for the tract.

Attachments

A_TH_CANYON_RANCH_LOMA_LINDA_LLC_Agreement.pdf
B_Attachment_A_-_Location_Map.pdf

RECORDING REQUESTED BY:
DEVELOPMENT SERVICES DEPARTMENT
CITY OF REDLANDS

WHEN RECORDED RETURN TO:
CITY CLERK'S OFFICE
CITY OF REDLANDS
P.O. BOX 3005
REDLANDS, CA 92373

(THIS SPACE FOR RECORDER'S USE ONLY)

CITY OF REDLANDS
AGREEMENT FOR OWNERSHIP AND MAINTENANCE OF FORCE SEWER MAIN AND PRIVATE LIFT STATION

THIS AGREEMENT FOR OWNERSHIP AND MAINTENANCE OF FORCE SEWER MAIN AND PRIVATE LIFT STATION (this "Agreement"), is made this 6th day of October, 2026, between the CITY OF REDLANDS, a California municipal corporation ("City") and TH CANYON RANCH LOMA LINDA LLC, a California limited liability company ("Developer"). City and Developer are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

RECITALS

WHEREAS, Developer owns real property commonly known as "Covenant Point" (the "Developer Property"), located within the City of Redlands, California, as more particularly described on Exhibit A attached hereto, and identified as Tract No. 20402 upon which Developer is developing and constructing a residential project (the "Project").

WHEREAS, Developer intends to construct and maintain a private sewer force main (the "Sewer Main") within the City's right-of-way of San Timoteo Canyon Road and Barton Road, which is located adjacent to the Property and within the area (the "Right of Way Area") shown on the Private Force Main Improvement Plans (City of Redlands Plan Number F-1876) on file with the City of Redlands (the "Force Main Improvement Plans"), and depicted on Exhibit B attached hereto.

WHEREAS, Developer coordinated with Proactive Engineering Consultants for preparation of a report titled "Private Sewer Lift Station and Force Main Engineering Design Report and Emergency Response Plan" dated November 26, 2025, (the "Design Report and Emergency Response Plan")

WHEREAS, Developer, in connection with the Project, has created or will create a homeowner's association (the "Association") to provide, among other things, for the maintenance of certain improvements and common areas of the Project, including the Sewer Main.

WHEREAS, Developer and the City desire to enter into this Agreement to provide for the continued maintenance of the Sewer Main by Developer and then the Association.

NOW, THEREFORE, in consideration of the mutual promises contained herein, the parties agree as follows:

1. Purpose. The purpose of this Agreement is to assure the ongoing maintenance of the Sewer Main within the Right of Way Area constructed by Developer for the benefit of houses within Tract 20402.

2. Developer's Duty to Maintain Sewer Main. Following Developer's construction of the Sewer Main until the Association accepts the obligation to inspect, maintain in good working order, repair and replace, as necessary, the Sewer Main, Developer shall maintain the Sewer Main in accordance with the Design Report and Emergency Response Plan and the City requirements set forth in City of Redlands Municipal Code Section 13.44.160: Private Sewer Laterals, as it may be modified or updated from time-to-time. Developer shall not be relieved of its obligation to maintain the Sewer Main as provided herein until the Association has been duly formed and the obligations hereunder have been fully assigned to the Association.

3. Association's Duty to Maintain Sewer Main. After completion of the Sewer Main and related pump station, Developer shall transfer or assign this Agreement ("Assignment") to the Association and the obligations of Developer under this Agreement, including the obligation to maintain the Sewer Main in accordance with the City of Redlands Municipal Code Section 13.44.160: Private Sewer Laterals, as it may be modified or updated from time-to-time. Upon such Assignment to Association, Association shall become the Developer under this Agreement and be obligated to perform all duties, covenants and obligations of Developer under this Agreement. Developer shall provide notice to City of the Assignment to the Association, which notice shall include the name of a designated contact person and notice address of the Association. Developer shall remain obligated to maintain the Sewer Main as provided in Section 2 above until the Association has been duly formed and all obligations hereunder have been fully assigned to the Association.

4. Breach and Remedies. If Developer breaches its obligations under this Agreement in any material respect, the City shall have all rights and remedies available at law or in equity, including, without limitation, the right to terminate this Agreement; provided, however, that the non-breaching party has given the breaching party notice of the applicable breach and the breaching party has failed to cure the breach of this Agreement within ten (10) days, for any breach that can be cured with the payment of money, or within thirty (30) days for any other breach; and provided, further, however, that if the applicable non-monetary breach is not reasonably susceptible of cure within such thirty (30) day period, and if the breaching party commences to cure the breach within such thirty (30) day period and thereafter diligently pursues such cure to completion, the breaching party shall have such additional time as is reasonably necessary to cure the applicable breach. In any legal action arising out of this Agreement, the substantially prevailing party shall be entitled to a reasonable sum for attorney's fees and court costs incurred.

5. Indemnification and Reimbursement of City. Developer shall indemnify and hold harmless City, its officers, directors, agents, employees, and invitees (each of which is an indemnitee) against and from any and all claims, losses, costs and expenses (including attorneys' fees), penalties, judgments, or obligations whatsoever for, or in connection with injury (including death), damage to any person, or loss or damage of property to whomsoever belonging, arising from Developer's ownership, operation, and/or maintenance of the Sewer Main. Developer shall reimburse City for any cost directly incurred by City to maintain or repair the Sewer Main or pump station that is caused by or is the result of the failure of Developer to properly maintain or repair the Sewer Main or due to the

City having to maintain or repair the Sewer Main due to Developer's negligence to maintain or repair the privately owned sewer facilities.

6. Notices. Any notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a party may provide notice in accordance with this section.

If to City: Development Services Department Director
City of Redlands
PO Box 3005
Redlands, CA 92373

With a Copy to: Municipal Utilities & Engineering Department Director
City of Redlands
PO Box 3005
Redlands, CA 92373

If to Developer: TH Canyon Ranch Loma Linda LLC
c/o Trumark Properties LLC
3001 Bishop Drive, Suite 100
San Ramon, CA 94583
Attn: Legal Department

7. Severability. The provisions of this Agreement are severable. If any portion of this Agreement is held invalid by a court of competent jurisdiction, the remainder of this Agreement shall remain in full force and effect unless amended or modified by mutual written consent of the Parties.

8. Captions. The captions of this Agreement are for convenience and reference only and shall not define, explain, modify, limit, exemplify, or aid in the interpretation, construction or meaning of any provisions of this Agreement.

9. Litigation. In the event that any action is commenced to enforce or interpret the terms of this Agreement the prevailing Party shall, in addition to costs and other relief, be entitled to litigation costs and reasonable attorneys' fees, including fees for use of in-house counsel by a Party.

10. Incorporation of Recitals. The recitals to this Agreement are hereby incorporated into the terms of this Agreement.

11. Entire Agreement. This Agreement constitutes the entire agreement of the Parties with respect to its subject matter. All modifications, amendments, or waivers of the terms of this Agreement must be in writing and signed by the appropriate representatives of the Parties.

12. Interpretation. This Agreement shall be governed by and construed in accordance with the laws of the State of California.

IN WITNESS WHEREOF, each party has executed and this Agreement effective on the date set forth above.

TH Canyon RANCH LOMA LINDA LLC CITY OF REDLANDS

By: _____ By:_____
Name, Title Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

(Notary attachment and proof of authorization
for all signatures required and must be attached)

EXHIBIT A

Legal Description of Developer Property

Real property in the City of Redlands, County of San Bernardino, State of California, described as follows:

Tentative Tract Map # 20402, in the City of Redlands, County of San Bernardino, State of California, APN #0293-132-01-0-000 & APN #0293-141-40-0-000.

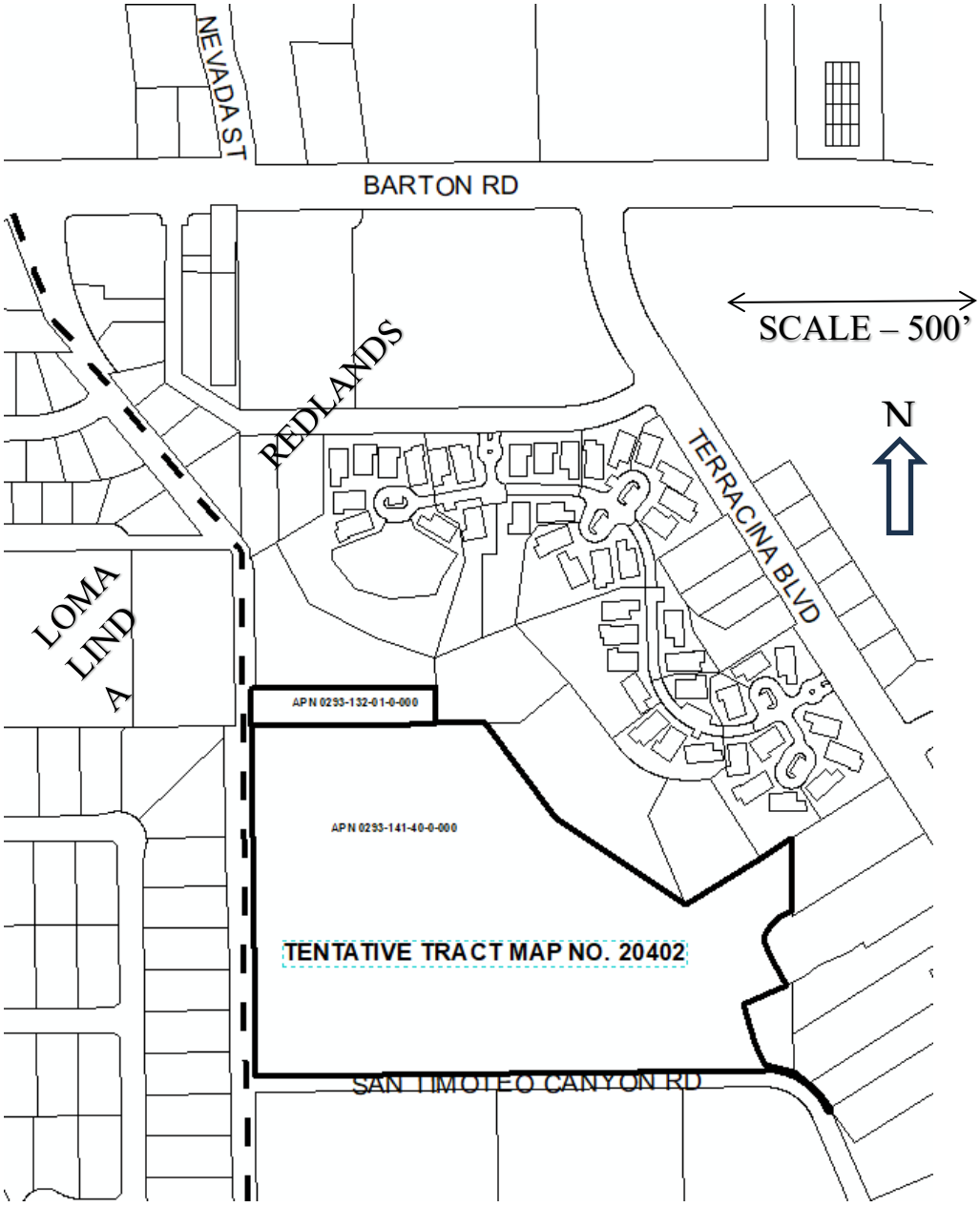


EXHIBIT B

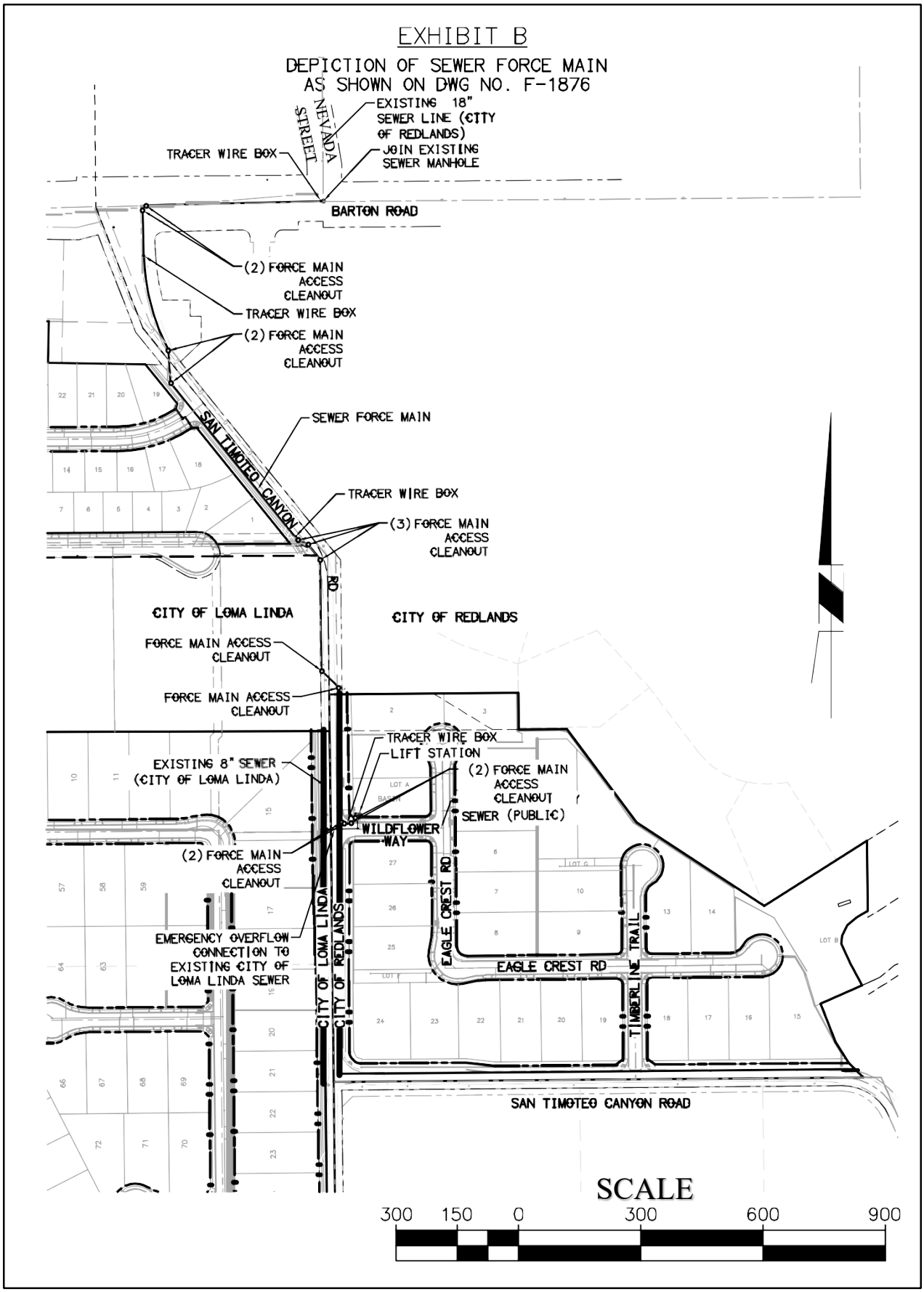
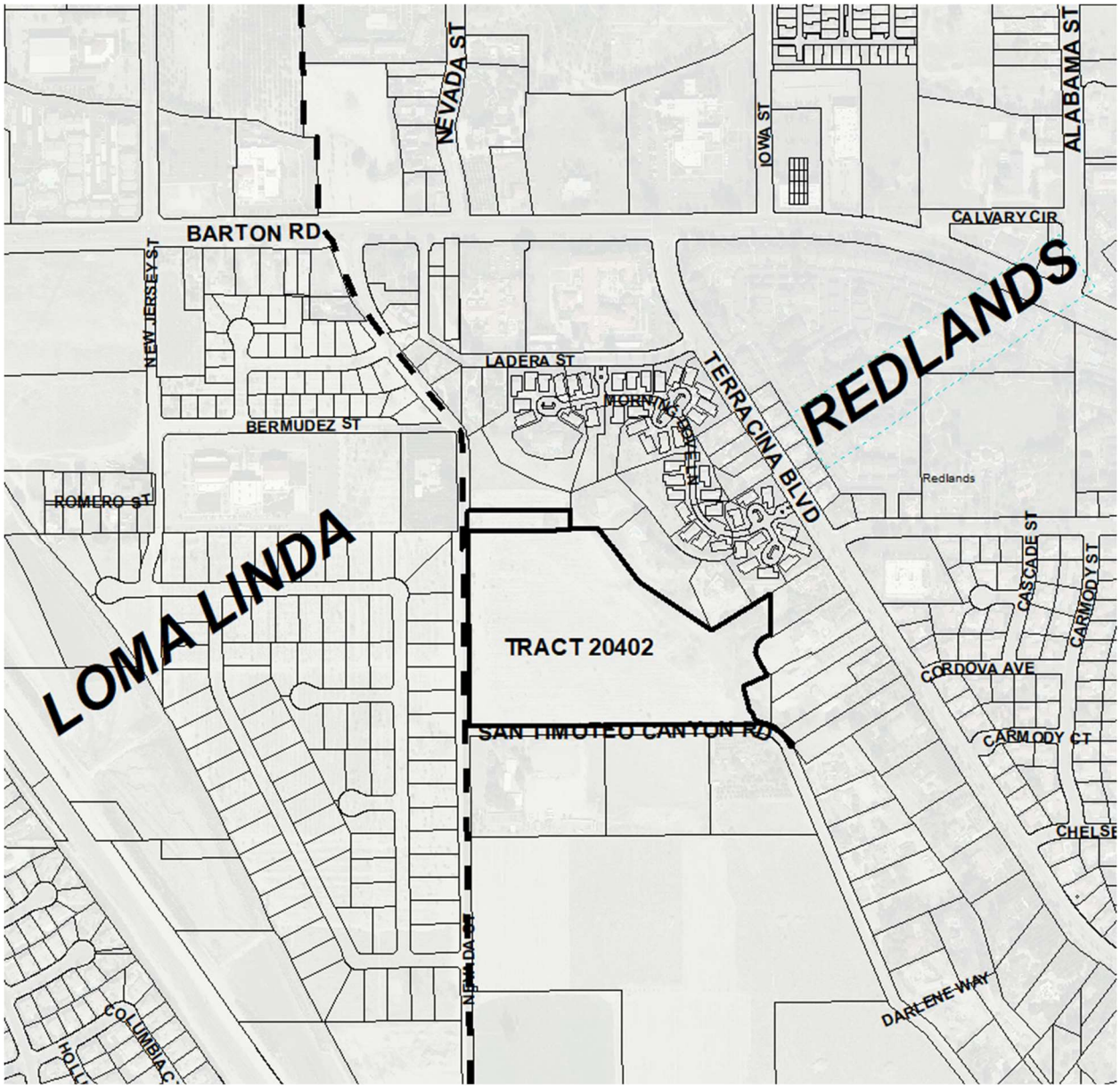


EXHIBIT B
DEPICTION OF SEWER FORCE MAIN
AS SHOWN ON DWG NO. F-1876
EXISTING 18" SEWER LINE (CITY OF REDLANDS)
JOIN EXISTING SEWER MANHOLE
NEVADA STREET
TRACER WIRE BOX
BARTON ROAD
(2) FORCE MAIN ACCESS CLEANOUT
TRACER WIRE BOX
(2) FORCE MAIN ACCESS CLEANOUT
SEWER FORCE MAIN
SAN TIMOTEO CANYON RD
TRACER WIRE BOX
(3) FORCE MAIN ACCESS CLEANOUT
CITY OF LOMA LINDA
CITY OF REDLANDS
FORCE MAIN ACCESS CLEANOUT
FORCE MAIN ACCESS CLEANOUT
TRACER WIRE BOX
LIFT STATION
(2) FORCE MAIN ACCESS CLEANOUT
SEWER (PUBLIC)
EXISTING 8" SEWER (CITY OF LOMA LINDA)
WILDFLOWER WAY
(2) FORCE MAIN ACCESS CLEANOUT
EMERGENCY OVERFLOW CONNECTION TO EXISTING CITY OF LOMA LINDA SEWER
CITY OF LOMA LINDA
CITY OF REDLANDS
EAGLE CREST RD
EAGLE CREST RD
TIMBERLINE TRAIL
SAN TIMOTEO CANYON ROAD
SCALE
300 150 0 300 600 900

ATTACHMENT A

LOCATION MAP



City Council **AGENDA ITEM NO. I10.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Adopt Resolution No. 8827 adopting the 2026 City of Redlands Emergency Operations Plan (Fire Chief Sessler)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council adopt Resolution No. 8827 adopting the updated City of Redlands Emergency Operations Plan and rescinding Resolution No. 6888.

RECOMMENDATION:

Staff recommends that the City Council adopt Resolution No. 8827 adopting the updated City of Redlands Emergency Operations Plan (EOP), which establishes the City's comprehensive framework for emergency preparedness, response, recovery, and mitigation activities; rescind Resolution No. 6888; and authorize implementation of the updated EOP in accordance with applicable federal, state, and local emergency management requirements.

DISCUSSION:

During Fiscal Year 2025–2026, the City of Redlands completed a comprehensive update to its Emergency Operations Plan (EOP) to ensure the plan reflects current emergency management best practices, the City's current organizational structure, and its evolving hazard profile. The City's existing EOP was adopted by Resolution No. 6888 on September 15, 2009, more than 17 years ago. Given the significant changes in emergency management practices, regulatory requirements, organizational structure, and the City's hazard environment since the existing plan was adopted, an updated EOP is necessary to ensure the City maintains a current and effective framework for emergency preparedness and response.

The updated EOP was developed through a collaborative effort between the City's emergency management team and its consultant, Jacob Green & Associates. The plan incorporates current planning standards established by the California Governor's Office of Emergency Services (Cal OES) and the Federal Emergency Management Agency (FEMA), as well as lessons learned and evolving best practices in emergency management.

The EOP is required under Redlands Municipal Code Chapter 2.52.150, which establishes the City's obligation to maintain a current emergency plan to provide for the effective mobilization and response to a disaster. Adoption of the updated EOP will ensure continued compliance with applicable state and federal preparedness requirements, including California Government Code Sections 8569 and 8610 and FEMA's *Comprehensive Preparedness Guide 101*.

Redlands faces a diverse hazard environment, including seismic activity, wildfire and smoke, extreme heat, flooding, transportation-related incidents, and hazardous materials events that require an adaptive and coordinated emergency response framework. The updated EOP provides that framework by defining roles, responsibilities, and operational procedures for City departments during extraordinary emergencies and disasters. It incorporates the concepts of operations required by the Incident Command System, California's Standardized Emergency Management System, and the National Incident Management System, ensuring the City can effectively integrate with county, regional, state, and federal response partners.

The updated EOP strengthens the City's ability to mobilize and manage emergency resources, supports coordinated interdepartmental operations, and provides City staff with clear procedures for emergency response and initial disaster recovery. Maintaining an adopted and current EOP is essential to operational readiness and supports the City's eligibility for certain state and federal emergency management grants.

Adoption of the updated EOP and rescission of Resolution No. 6888 will:

- Demonstrate the City's ongoing commitment to proactive emergency preparedness;
- Replace the City's existing 2009 EOP with a current and comprehensive emergency management framework;
- Provide a unified operational framework for City departments during emergencies;
- Ensure alignment with county, state, and federal emergency management systems;
- Support coordinated disaster response, effective communication, and efficient resource management; and
- Ensure the City's emergency planning framework remains consistent with current hazards, emergency management standards, and best practices.

Following adoption, as directed by the City Manager, the City's emergency management staff will maintain and periodically update the EOP as necessary to ensure continued compliance with state and federal standards and alignment with emerging hazards, organizational changes, and evolving emergency management best practices.

ALTERNATIVES:

The City may choose not to adopt the updated Emergency Operations Plan and provide direction to staff regarding any revisions or additional information the City Council wishes to consider prior to adoption.

STRATEGIC PLAN:

Priority B - Public Health & Safety

SUBMITTED BY:
Rich Sessler, Fire Chief

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Bruni Reyes, Management Analyst
Bruni Reyes, Management Analyst

FISCAL IMPACT

Fiscal Year:

Revenue Generating: No

Amount: $

Budgeted Y/N:

Account No.:

Additional Appropriation Required: Yes or No

Discussion:

There is no direct fiscal impact associated with the adoption of the updated City of Redlands Emergency Operations Plan (EOP). The EOP serves as the City's operational framework for emergency preparedness, response, recovery, and mitigation activities. Any costs associated with implementing specific emergency management initiatives, training, exercises, equipment, or emergency response activities will be addressed through existing departmental budgets, future budget appropriations approved by the City Council, and, when applicable, reimbursement opportunities through state and federal disaster assistance or grant funding.

Attachments

A_Resolution_No_8827_EOP.pdf
B_Exhibit_A_-_EOP_With_Director_signature.pdf
C_Rescinded_Resolution_No_6888_Emergency_Operation_Plan.pdf
B_Exhibit_A_-_EOP_With_Director_signature_1.pdf

RESOLUTION NO. 8827

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS RESCINDING RESOLUTION NO. 6888 AND ADOPTING THE 2026 EMERGENCY OPERATIONS PLAN

WHEREAS, the City of Redlands recognizes the importance of emergency preparedness to protect life, property, and the environment; and

WHEREAS, California Government Code Sections 8569 and 8610, and Chapter 2.52.150 of the City of Redlands Municipal Code, require the City to maintain and adopt an Emergency Operations Plan; and

WHEREAS, on November 18, 2025, the City retained Jacob Green and Associates (JGA) to update and develop the City's Emergency Operations Plan (EOP) to ensure consistency with current state and federal guidelines and to provide an effective tool for the City's response to emergency situations; and

WHEREAS, the Emergency Operations Plan has been prepared in alignment with the California Office of Emergency Services (CalOES) guidance and the Federal Emergency Management Agency's (FEMA) Comprehensive Preparedness Guide 101; and

WHEREAS, the plan, as developed, incorporates the requirement of the Standardized Emergency Management System (SEMS) as prescribed by the State of California and the National Incident Management System (NIMS) as prescribed by FEMA; and

WHEREAS, the updated EOP reflects the City's evolving hazard profile, including fires, severe weather, flooding, seismic risks, and provides a comprehensive framework for effective disaster response, recovery and coordination with local, county, state and federal partners; and

WHEREAS, adoption of the EOP by the City Council will enable the City to coordinate emergency response more effectively with other levels of government, support resource sharing during disasters, and comply with state and federal emergency planning requirements; and

WHEREAS, the City Council has reviewed the Emergency Operations Plan and finds that it supports the City's commitment to preserving and protecting the quality of life for residents and businesses while ensuring a sustainable and resilient future.

NOW, THEREFORE, be it resolved by the City Council of the City of Redlands as follows:

Section 1. The City Council of the City of Redlands hereby adopts the 2026 Emergency Operations Plan (EOP), attached hereto as Exhibit "A," as the official Emergency Operations Plan of the City of Redlands. The 2026 EOP establishes the City's comprehensive framework for emergency preparedness, response, recovery and coordination during disasters and other emergency situations and shall be implemented in accordance with applicable federal, state and local laws, regulations and emergency management requirements.

Section 2**.** The City Manager, or designee, is authorized and directed to implement the 2026 Emergency Operations Plan and to take such actions as may be necessary and appropriate to maintain the Plan in accordance with applicable federal, state, and local requirements. The EOP shall be reviewed and updated as necessary to reflect changes in laws, regulations, hazards, operational requirements and best practices. Upon adoption of the 2026 EOP, it shall supersede and replace the City's previously adopted Emergency Operations Plan.

Section 3. Resolution No. 6888 is hereby rescinded.

Section 4. This Resolution shall become effective immediately upon its adoption.

ADOPTED, SIGNED AND APPROVED this 6th day of October, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, Deputy City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, hereby certify that the foregoing resolution was duly adopted by the City Council at a regular meeting thereof held on the 6th day of October, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

EXHIBIT “A”

2026 Emergency Operations Plan

EMERGENCY OPERATIONS PLAN

A STRATEGY FOR THE CITYWIDE RESPONSE TO MAJOR EMERGENCIES AND DISASTERS

JULY 2026

Portions of the Emergency Operations Plan, including supporting parts and annexes, may contain sensitive information related to the deployment, mobilization, and tactical operations of the City of Redlands government and cooperating or assisting agencies in response to emergencies.

While the EOP Base Plan (Part 1) is available for public use and review, the City may withhold certain supporting parts and annexes from full public disclosure under the provisions of the California Public Records Act (California Government Code § 7920-7931).

PROMULGATION STATEMENT

This **Emergency Operations Plan** is adopted as the official emergency plan of the City of Redlands by Resolution No. 8827 of the City of Redlands City Council, California, dated October 6, 2026. This version supersedes all previous versions.

_____

MARIO SAUCEDO, MAYOR

City of Redlands

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Preface **9**

Concurrence Signatures to the Emergency Operations Plan **17**

Plan Organization and Activation **19**

Plan Organization 19

Plan Activation 19

Triggering Events 20

Preemptive Response Actions 20

How to Use This Plan 21

1. Purpose and Scope **23**

1.1 Purpose 23

1.2 Scope 23

1.3 Basis for Planning 24

1.4 Response Objectives 24

2. Situation and Assumptions **25**

2.1 Situation Overview 25

2.2 Hazards Summary 26

2.3 Planning Assumptions 28

3. Concept of Operations **29**

3.1 General Overview 29

3.2 Phases of Emergency Management 29

3.3 Standardized Emergency Management System 34

3.4 National Incident Management System 36

3.5 Incident Command System 36

3.6 Emergency Support Functions 37

3.7 Emergency Proclamations 37

3.8 Operating Conditions 39

3.9 EOC Activation and Deactivation 41

3.10 EOC Activation Levels 43

3.11 EOC Staffing Matrix for City Departments 47

3.12 EOC Action Plans....47
3.13 Cultural Competence....48
3.14 Disabilities or Access and Functional Needs Populations....48
3.15 Animal Care Considerations....49
3.16 Recovery Organization....50
3.17 Recovery Operations....50
3.18 Emergency Facilities....59
4. Organization and Assignment of Responsibilities....63
4.1 City Level....63
4.2 Operational Area Level....66
4.3 Regional Level....67
4.4 State Level....67
4.5 Federal Level....67
4.6 External Partners....68
5. Direction, Control, and Coordination....73
5.1 Director of Emergency Services....73
5.2 City EOC....73
5.3 City Department Direction....73
5.4 Department Operations centers....73
5.5 Local Control....73
5.6 On-Scene Control....74
5.7 Coordination and Interface....74
6. Information Collection, Analysis, and Dissemination....79
6.1 Objectives....79
6.2 Information Collection....80
6.3 Analysis and Dissemination....82
7. Communications....85
7.1 Public Alert and Warning....85
7.2 Communication Systems....90
7.3 Public Information....93

8. Mutual Aid and Resource Management 95
8.1 Mutual Aid Overview 95
8.2 Mutual Aid Agreements 95
8.3 California Mutual Aid Framework 96
8.4 City Mutual Aid Participation 100
8.5 Emergency Management Assistance Compact 102
8.6 Resource Management Overview 103
9. Continuity of Government 107
9.1 Reconstitution of Government 107
9.2 Director of Emergency Services 108
9.3 Succession of Officers 109
9.4 Alternate Seat of Government 110
9.5 Preservation of Vital Records 110
10. Administration, Finance, and Logistics 113
10.1 Administrative Practices 113
10.2 Documentation 113
10.3 Finance During Disasters 114
10.4 Logistics 115
11. Training and Exercise 117
11.1 Emergency Operations Training 117
11.2 Emergency Operations Exercises 118
12. Plan Development and Maintenance 121
12.1 Plan Development 121
12.2 Plan Maintenance 122

Appendices

Appendix A: Resolution of EOP Adoption
Appendix B: Authorities and References
Appendix C: Abbreviations and Acronyms
Appendix D: Glossary of Terms
Appendix E: EOC Staffing Matrix
Appendix F: Emergency Support Functions Crosswalk

THIS PAGE IS INTENTIONALLY LEFT BLANK

PREFACE

EOP OVERVIEW

The City of Redlands Emergency Operations Plan (EOP) outlines the concepts and strategies used to prevent, mitigate, prepare for, protect against, respond to, and recover from natural, technological, and human-caused hazards that could impact the City. All actions described in the EOP are focused on protecting life, property, and the environment; maintaining essential government operations; and supporting a timely transition to recovery. The EOP is developed with an emphasis on coordination, collaboration, and cooperation.

EOP DEVELOPMENT

The EOP has been developed in accordance with the California Standardized Emergency Management System (SEMS) and the National Incident Management System (NIMS). The EOP is written in coordination with the State of California Emergency Plan, the National Response Framework, and FEMA's "Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans".

The City of Redlands the Disaster Council is responsible for developing "emergency and mutual aid plans and agreements" (City of Redlands Municipal Code (MC) MC § 2.52.060). The Emergency Plan (MC § 2.52.150) is developed to "provide for the effective mobilization of all of the resources of the City, both public and private, to meet any condition constituting a local emergency, state of emergency, or state of war emergency."

The City Manager, as the Director of Emergency Services, is empowered to "control and direct the effort of the emergency organization of the City" (MC § 2.52.100) and is ultimately responsible for directing disaster readiness, emergency planning, and response and recovery efforts.

This plan provides the framework within which City departments, special districts, allied agencies, non-governmental organizations, volunteer groups, and private organizations can develop detailed response procedures, continuity of government/continuity of operations plans, resource arrangements, and aid agreements. These departments, agencies, and organizations collectively comprise the City of Redlands Emergency Organization (MC § 2.52.140).

EOP ORGANIZATION

To ensure the greatest flexibility, the EOP is organized in parts focusing on specific emergency management areas. City departments may develop and maintain standard operating procedures (SOPs) as needed to support their role in the EOP.

The EOP consists of five parts:

1. Part 1: Base Plan
2. Part 2: Emergency Operations Center (EOC) Position Checklists
3. Part 3: Functional Annexes
4. Part 4: Hazard-Specific Annexes
5. Part 5: Supporting Attachments

While some parts of the EOP are complete, others may be under development, in the revision process, or scheduled for future planning efforts.

EOP SUPPORTING PROCEDURES

Recipients of this EOP are responsible for developing detailed plans, procedures, agreements, and arrangements specific to their departments or agencies. They must ensure personnel are trained to implement these measures and make updates as needed. Departments or agencies assigned responsibilities under this plan should have access to the emergency resources identified in the plan, as well as the ability to obtain those resources during an emergency or disaster.

EOP UPDATES

Emergency planning is a continuous, cyclical process and the EOP will be regularly reviewed and updated to reflect changes. Revisions may be made based on lessons learned from real-world incidents and exercises; advancements in technology; new laws or regulations; organizational changes within the jurisdiction; and shifts in local or partner agency capabilities. The City will issue supplements to this plan as needed to address specific hazards, specialized emergency functions, or complex planning issues. Regular and routine updates may be made without further promulgation or legislative action.

SUMMARY

While no plan can fully prevent the loss of life or damage to property, well-developed plans carried out by trained and knowledgeable personnel can help minimize these losses. City departments, allied agencies, non-governmental organizations, volunteer groups, and private entities are encouraged to take all necessary preparedness actions to fulfill their roles in the EOP.

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECORD OF CHANGES

DATE	CHANGE NO.	PART, ANNEX, OR ATTACHMENT CHANGED	PERSON MAKING CHANGE

THIS PAGE IS INTENTIONALLY LEFT BLANK

PLAN DISTRIBUTION	
DEPARTMENT / AGENCY / ORGANIZATION	
City of Redlands City Manager's Office	City of Redlands City Attorney's Office
City of Redlands City Clerk's Office	City of Redlands Fire Department
City of Redlands Management Services/Finance Department	City of Redlands Police Department
City of Redlands Human Resources Department	City of Redlands Municipal Utilities & Engineering Department
City of Redlands Facilities & Community Services Department	City of Redlands Development Services Department
City of Redlands EOC (Primary)	City of Redlands Library
City of Redlands EOC (Alternate)	

DISTRIBUTION METHODOLOGY

- All planning documents will be distributed digitally.
- Part 1 Base Plan will be distributed upon promulgation.
- All other EOP components—including attachments, annexes, and appendices—will be distributed as they are developed, updated, or revised.

THIS PAGE IS INTENTIONALLY LEFT BLANK

CONCURRENCE SIGNATURES TO THE EMERGENCY OPERATIONS PLAN

City Manager/Director of Emergency Services

Assistant City Manager

Assistant City Manager

City Attorney

City Clerk

Fire Chief

Police Chief

Director, Management Services/Finance Department

Director, Municipal Utilities & Engineering Department

Director, Human Resources Department

Director, Facilities & Community Services Department

Director, Development Services Department

Director, Library

Concurrence indicates agreement with
the general concept of operations of the plan
and department, agency, or organization assigned tasks.

THIS PAGE IS INTENTIONALLY LEFT BLANK

PLAN ORGANIZATION AND ACTIVATION

PLAN ORGANIZATION

The EOP is divided into five distinct parts to enhance its usability and flexibility for emergency personnel and key City officials.

PART 1: BASE PLAN

Authorities, concept of operations, and assignment of responsibilities.

PART 2: EOC POSITION CHECKLISTS

EOC activation procedures, organization, and functional position descriptions.

PART 3: FUNCTIONAL ANNEXES

Standard operating concepts and procedures for commonly required EOC emergency response and support functions.

PART 4: HAZARD-SPECIFIC ANNEXES

Standard operating concepts and procedures that are unique to specific hazards and threats.

PART 5: SUPPORTING ATTACHMENTS

Reserved for supporting documents and references essential to the execution of the jurisdictional EOP and not fitting into Parts 2-4.

While some parts of the EOP are complete, others may be under development, in the revision process, or scheduled for future planning efforts.

PLAN ACTIVATION

The plan will become activated:

- By order of the City Manager as the Director of Emergency Services, or the Assistant City Manager, or the Fire Chief, or the Chief of Police, or a Department Director, or a designee, or
- Upon the proclamation of a local emergency or when conditions exist that may warrant such a proclamation, consistent with the authority granted in MC § 2.52.100, or

- When the Governor has proclaimed a State of Emergency in an area, including the City of Redlands, or
- At the proclamation of a State of War Emergency, as defined by the California Emergency Services Act, or
- Upon a Triggering Event identified within this section.

In the event of a threatened emergency, all or part of the City's Emergency Organization (MC § 2.52.140) may be mobilized—even before this plan is formally activated—by order of the City Manager, Assistant City Manager, Fire Chief, Chief of Police, a Department Director, or a designee.

TRIGGERING EVENTS

The following events may trigger the activation of the EOP and EOC:

- Damaging earthquake, wildfire, flood, or other impactful event
- Severe weather warning
- Significant commitment or draw-down of City emergency resources
- Regularly scheduled emergency exercises or training activities
- City-sponsored special events of extraordinary significance
- Any incident that inhibits the City's ability to deliver essential services
- Any situation in which City resources are overwhelmed, and a coordinated response is required to protect life, property, or public safety

PREEMPTIVE RESPONSE ACTIONS

Prior to a potential, impending, or threatened emergency, actions will be taken to prevent an incident, reduce its impact, or enhance City readiness. These actions may include but are not limited to gathering and maintaining situational awareness and resource status information; pre-alerting response departments and partner organizations; developing incident-specific contingency plans and staffing strategies; pre-positioning response assets and emergency supplies; and establishing and maintaining communication with Department Directors, assisting and cooperating agencies, and the City's Emergency Organization.

Preemptive response actions may be ordered by the City Manager, Assistant City Manager, Fire Chief, Chief of Police, a Department Director, or a designee.

HOW TO USE THIS PLAN

Prior to EOP Activation

- Understand departmental or organizational responsibilities
- Develop all necessary supporting Standard Operating Procedures (SOPs)
- Acquire and allocate resources necessary to fulfill assigned responsibilities
- Train staff and teams to perform their roles as outlined in the EOP or SOPs

Upon EOP Activation

- Refer to the EOC organizational chart in EOP Part 2 (Position Checklists)
- Identify the function for which your department or organization is responsible and ensure it is staffed within the City's EOC
- Locate the corresponding section in EOP Part 2 that outlines the function and associated tasks
- Under the direction of the Director of Emergency Services/EOC Director, carry out the functions and associated tasks consistent with the EOC Action Plan or stated incident priorities

THIS PAGE IS INTENTIONALLY LEFT BLANK

1. PURPOSE AND SCOPE

1.1 PURPOSE

This plan outlines the actions to be taken by the City to prevent disasters where possible, reduce vulnerability, protect people and property, respond effectively, and recover from extraordinary emergencies and disasters.

The Emergency Operations Plan (EOP) serves as the primary guide for the City's Emergency Organization, outlining procedures to effectively plan, prepare for, and respond to emergencies.

1.2 SCOPE

The City's EOP uses an all-hazards approach to outline its planned response to extraordinary emergencies caused by natural disasters and human-caused incidents. While it does not address routine, day-to-day emergencies, the plan focuses on large-scale disasters and catastrophic incidents that may create unique situations requiring a significant response. The Base Plan establishes authority and provides a foundational concept of operations upon which further plans, procedures, guidelines, arrangements, and agreements can be built.

The EOP is designed to be adaptable, supporting any emergency or disaster affecting the City. It prioritizes initial response efforts on saving lives, protecting property, and meeting basic human needs in the immediate aftermath of an emergency or disaster. Additionally, the plan guides the restoration of affected areas to normalcy and helps mitigate further harm or damage during recovery efforts.

The EOP applies to all City departments and external entities that may assist in an emergency or disaster. Departments can respond within their own authorities and capabilities or as part of a coordinated citywide effort. References to City departments include divisions and organizational units, while non-governmental and quasi-governmental organizations (e.g., school districts, telecommunications providers, universities, and volunteer groups) may also play a supporting role in response and recovery efforts.

1.3 BASIS FOR PLANNING

California Government Code § 8568 states: "The State Emergency Plan shall be in effect in each political subdivision of the state, and the governing body of each political subdivision shall take such action as may be necessary to carry out the provisions thereof."

United States Homeland Security Presidential Directive-5 (HSPD-5) directs the development and implementation of the National Incident Management System (NIMS). NIMS requires developing and maintaining various planning elements at the local government level, including the EOP.

The City EOP is developed in accordance with the MC § 2.52.150 and takes effect upon adoption by resolution of the City Council.

1.4 RESPONSE OBJECTIVES

The following objectives guide the planning and the conduct of response and recovery efforts for the City during an emergency:

- Protect lives
- Provide for the continuity of government
- Safeguard property, the environment, and the economy
- Repair and restore essential systems, services, and lifelines
- Provide a basis for direction and control of emergency operations
- Provide for the protection, use, and distribution of emergency resources
- Coordinate emergency operations with other jurisdictions and emergency service organizations.

2. SITUATION AND ASSUMPTIONS

2.1 SITUATION OVERVIEW

History: Redlands was incorporated in 1888 after attracting eastern and midwestern settlers who shaped it into a cultural, educational, and agricultural community. Founded by Frank E. Brown and E. G. Judson, the City grew around citrus—especially the Washington navel orange—earning recognition as the "Navel Orange Capital of the World." Philanthropic leaders including Alfred H. and Albert K. Smiley, Clarence G. White, and Robert Watchorn established lasting cultural landmarks, reinforcing Redlands' reputation as the "Jewel of the Inland Empire." The City prospered through the early 20th century with citrus agriculture, the University of Redlands, and Norton Air Force Base, though the base's 1994 closure and the economic downturn beginning in 1990 challenged its stability.

Location: Redlands is located in San Bernardino County within Southern California's Inland Empire, positioned at the base of the San Bernardino Mountains. The City is located approximately 63 miles east of Los Angeles and spans 36.25 square miles. Redlands shares borders with the communities of Highland, Mentone, Crafton, Yucaipa, Loma Linda, and portions of San Bernardino. Its elevation averages 1,358 feet above sea level, placing it at a natural transition zone between the urbanized Inland Empire and the mountain and desert corridors to the east.

Climate: The City has a Mediterranean climate, characterized by mild, wet winters and warm, dry summers. Temperatures are generally moderate to warm throughout the year, with average highs ranging from 67°F in winter to 96°F in summer. The City averages 12.9 inches of rainfall per year.

Demographics: According to 2025 U.S. Census estimates, the City's population is approximately 74,128. The three largest racial/ethnic demographic groups in the City are White (47.9%), Hispanic/Latino (39.5%), and Asian (8.6%). Approximately 30.1% of the population speaks a language other than English at home.

City Services: The City of Redlands is a general law city operating under a council-manager form of government. The City provides its own police and fire protection services through the Redlands Police Department and the Redlands Fire Department. The City also operates a general aviation airport, maintains a municipal animal shelter, and manages its own water utility.

2.2 HAZARDS SUMMARY

2.2.1 CITY HAZARDS

A hazard is an event or condition that can cause fatalities, injuries, property and infrastructure damage, environmental harm, business disruptions, or other adverse impacts. Through the City's most recent hazard mitigation planning process (2021), the City evaluated natural, technological, and human-caused hazards that—regardless of likelihood—could affect City services and operations. The 2021 City of Redlands Local Hazard Mitigation Plan (LHMP) considered the 17 hazards listed in Table 2.2.1 City Hazards below.

Table 2.2.1 City Hazards

City Hazards	
Aircraft Accident/Incident	Infectious Disease
Civil Disturbance	Infestation
Dam Breach	Landslide
Drought	Technology Disruption
Earthquake	Terrorism
Energy Shortage/Power Outage	Train Accident/Incident
Extreme Temperature	Wildfire
Flood	Windstorm
Hazardous Material Accident	

Source: 2021 City of Redlands Local Hazard Mitigation Plan (LHMP)

2.2.2 COUNTY HAZARDS

San Bernardino County identified 18 hazards in its 2022 Multi-Jurisdictional Hazard Mitigation Plan (MJHMP), listed in Table 2.2.2 County Hazards on the next page. The hazards are ranked based on their probability of occurrence and potential impact.

Table 2.2.2 County Hazards

County Hazards	
Hazards	**Probability/Impact**
Climate Change	Medium Probability/Medium Impact
Dam Inundation	Low Probability/Medium Impact
Drought	High Probability/Medium Impact
Earthquake/Geologic Hazards	High Probability/High Impact
Extreme Heat	Medium Probability/Low Impact
Extreme Cold	Low Probability/Low Impact
Flood	High Probability/High Impact
Hazardous Waste	Probability/Impact Not Assessed
High Winds/Straight Line Winds	Low Probability/Low Impact
Hail	Medium Probability/Low Impact
Infestation	Medium Probability/Low Impact
Landslide	Medium Probability/Medium Impact
Lightning	Low Probability/Low Impact
Terrorism	Medium Probability/High Impact
Tornado	Low Probability/Low Impact
Volcanic Activity	Probability/Impact Not Assessed
Wildfire	High Probability/High Impact
Winter Storm/Heavy Snowfall	Low Probability/Low Impact

Source: 2022 San Bernardino County Multi-Jurisdictional Hazard Mitigation Plan (MJHMP)

2.2.3 COUNTY DISASTERS

San Bernardino County experienced 35 Federal Major Disaster Declarations between 1965 and 2020, including 13 fires, 18 severe weather events, one pandemic declared twice, and two earthquakes. During this same period, the County also received 20 Fire Management Assistance Declarations, beginning in 2003 (2025 SBCO EOP; 2022 SBCO MJHMP).

2.3 PLANNING ASSUMPTIONS

Planning assumptions establish the conditions the City accepts as factual for planning purposes, enabling effective execution of the EOP and facilitating decision-making when information is limited or uncertain. Planning assumptions include:

- Major emergencies and disasters will require a multi-agency, multi-jurisdictional response
- Major emergencies and disasters may require an extended commitment of personnel and other resources from involved agencies and jurisdictions
- Major emergencies and disasters may overburden local resources and necessitate mutual aid assistance
- Mutual aid assistance, critical equipment, essential supplies, and technical expertise may be limited or unavailable during regional or national disasters
- Major emergencies and disasters may pose serious long-term threats to public health, property, the environment, and the local economy
- Effective use of alert and warning systems reduces loss of life and property
- Vulnerable critical facilities have been identified and secured to protect life, personnel, equipment, and infrastructure
- The City maintains an EOC to manage all emergency management activities during major emergencies and disasters
- City departments develop and maintain internal operations plans and standard operating procedures that support this EOP
- The City conducts regular training and exercises to test the EOP and trains staff, using after-action reviews to drive continuous improvement
- Staff responsible for EOP implementation and disaster response have reviewed, exercised, and updated the Base Plan, Annexes, and SOPs, and are familiar with their roles
- Staff responsible for EOP implementation and disaster response have been trained in SEMS and NIMS and possess a full working knowledge of both systems
- City departments have integrated SEMS and NIMS into preparedness planning and apply both systems during disaster response operations

3. CONCEPT OF OPERATIONS

3.1 GENERAL OVERVIEW

The functions performed by City departments during emergency operations generally align with their normal functions. Tasks and operations that do not contribute directly to the emergency may be suspended or redirected during an emergency or disaster, and efforts that would typically be assigned to those tasks will be redirected toward emergency and disaster relief efforts.

If the emergency exceeds the City's capability to manage, assistance may be requested from San Bernardino County and the State. If the emergency exceeds the State's capability to manage, assistance may be requested from the Federal government.

This section of the plan outlines how the plan will be activated and implemented, with the purpose of protecting lives, property, and the environment of the City.

3.2 PHASES OF EMERGENCY MANAGEMENT

Emergency management consists of interrelated phases or mission areas that encompass activities before, during, and after a disaster; however, not every disaster necessarily includes all indicated phases. The Mitigation, Prevention, and Protection phases are combined for the purposes of this section.

All City departments have responsibilities in all phases.

3.2.1 PREPAREDNESS

The Preparedness phase consists of activities carried out before an emergency or disaster to build operational capabilities and ensure effective response. Preparedness activities include:

- Mitigation activities
- Emergency/disaster planning
- Training and exercises
- Public education on preparedness

Disaster plans are reviewed to guide response operations and maximize available resources. Planning activities include conducting hazard analyses, training response personnel, and enhancing public information and communication systems. Critical

facilities implement final preparations, additional staff and resources are mobilized, and warning systems are used both for testing and to inform staff of ongoing efforts.

3.2.1.1 COMMUNITY PREPAREDNESS

Public awareness and education are foundational to building community resilience from the ground up, empowering individuals and neighborhoods to sustain themselves during emergencies until first responders are able to provide assistance.

The City offers the following resources to enhance community preparedness:

- Community Emergency Response Team (CERT) Training
- Emergency Alerts
- Emergency Services
- Redlands Emergency Communications Group

San Bernardino County offers the following resources to enhance community preparedness:

- Emergency Alerts
- Preparedness Resources
- Volunteer Programs
- Listos (Spanish Language Resources)

3.2.2 MITIGATION/PREVENTION/PROTECTION

Mitigation, prevention, and protection strategies reduce disaster risks and impacts. Mitigation minimizes long-term risks, prevention avoids disasters, and protection safeguards people, property, and infrastructure.

3.2.2.1 MITIGATION

Mitigation reduces long-term risks to life and property from hazards. Mitigation efforts include amending local ordinances and statutes, such as zoning ordinances, building codes, and other enforcement codes; initiating structural retrofitting measures; assessing tax levies or abatements; emphasizing public education and awareness; undertaking flood control projects; removing fuel in areas with a high potential for wildfires; and assessing and altering land use planning.

3.2.2.2 PREVENTION

Prevention involves proactive measures to avoid or reduce disasters, such as enforcing safety regulations, conducting hazard assessments, and promoting public awareness. This helps prevent disruptions and minimize impacts. By focusing on prevention, the City can better prepare for threats and reduce vulnerabilities to various hazards.

3.2.2.3 PROTECTION

Protection safeguards people, property, and critical infrastructure from threats and hazards. It includes security measures around facilities, comprehensive emergency response plans, and robust communication and monitoring systems. Securing critical infrastructure enhances preparedness and aims to maintain continuous uninterrupted essential services.

3.2.3 RESPONSE

The Response phase includes any action taken before, during, or after an emergency situation to save lives, minimize damage to property, and enhance the effectiveness and speed of recovery. The response phase can be divided into:

- Pre-emergency response
- Emergency response

3.2.3.1 PRE-EMERGENCY RESPONSE

When a disaster is inevitable, actions are precautionary and emphasize protection of life. Typical responses might be:

- Review NIMS and SEMS SOPs
- Develop procedures for mobilizing public safety personnel and repositioning resources and equipment
- Develop a process for managing incidents using the Incident Command System (ICS) in coordination with the Police Department and Fire Department
- Notify and brief the City Manager and senior staff as appropriate
- Evacuate threatened populations to safe areas
- Alert populations by Rave Alert, City website, social media, radio, television, etc. and advise them on safety measures to be implemented

- Identify and request mutual aid
- Coordinate with the City Manager's Office on the process and procedure for activating Citizen Emergency Response Team (CERT) members and recruiting volunteers and additional staff (including the procedure for registering them as Disaster Service Workers)
- Review maps of specific hazards (e.g., hazmat, flood inundation areas, earthquake faults) to be used by City departments and emergency responders
- Prepare to mobilize CERT-trained personnel, auxiliary, and volunteer staff
- Pre-position resources and equipment
- Request a local emergency proclamation

3.2.3.2 EMERGENCY RESPONSE

During this phase, emphasis is placed on saving lives and property, controlling the situation, and minimizing the impacts of the emergency or disaster. Immediate response is accomplished by the City through timely and effective deployment. One of the following conditions will apply during this phase:

- The incident can be managed by the City
- The City requires mutual aid
- The City can provide mutual aid either locally or through the San Bernardino County Operational Area (OA)

The City will give priority to the following operations:

- Dissemination of accurate and timely alerts and warnings to the public
- Situation analysis
- Resource prioritization, allocation, and control
- Evacuation and rescue operations
- Medical care operations
- Mass care (i.e., reception, feeding, and shelter operations)
- Access and perimeter control
- Public health operations

- Restoration of vital services and utilities
- Multi-agency coordination

When local resources are insufficient, the City will use established mutual aid agreements and, if needed, request mutual aid through the appropriate San Bernardino County Mutual Aid Coordinator or the San Bernardino County OA EOC. More information about mutual aid is provided in **Section 8: Mutual Aid and Resource Management** of this EOP.

Depending on the emergency's severity, the San Bernardino County OA EOC may activate to support operations. If a State of Emergency is declared, State agencies will assist as coordinated by Cal OES, which may activate the State Operations Center (SOC) in Sacramento. The Cal OES Southern Region in Los Alamitos will support the San Bernardino County OA EOC. If a Presidential Declaration is granted, a State Coordinating Officer (SCO) will be appointed to manage recovery efforts with Federal agencies.

3.2.4 RECOVERY

Recovery operations establish procedures for accessing government programs that provide individual and public assistance after a disaster. Recovery may extend well beyond the conclusion of an emergency to restore normalcy, secure disaster response funding, and incorporate lessons learned into future preparedness and mitigation efforts. Short-term recovery focuses on damage assessment and restoring critical life-support systems to minimum operating levels. Long-term recovery and community rebuilding efforts may continue for many years.

Figure 3.2.4 below represents the disaster recovery process.

Figure 3.2.4 Disaster Recovery Process

Source: FEMA National Disaster Recovery Framework, 2024

Recovery Operations are further detailed in **Section 3.17: Recovery Operations** of this EOP.

3.3 STANDARDIZED EMERGENCY MANAGEMENT SYSTEM

The City has fully adopted the California Standardized Emergency Management System (SEMS), which is required by the California Government Code § 8607(a) for managing multiagency and multijurisdictional responses to emergencies in California. In times of emergency or disaster, the City will coordinate with other cities, San Bernardino County, the State, and the Federal government.

SEMS unifies all elements of California's emergency management community into a single integrated system and standardizes key elements. SEMS incorporates the use of the Incident Command System (ICS), California Disaster and Civil Defense Master Mutual Aid Agreement, the OA concept, and multiagency coordination. State agencies are required to use SEMS, and local government entities must use SEMS to be eligible for any reimbursement of response-related costs under the State's disaster assistance programs.

Unified Command (UC) allows multiple agencies with responsibility for an incident to manage an incident by establishing a common set of incident objectives and strategies. This is accomplished without losing or abdicating agency authority, autonomy, responsibility, or accountability.

3.3.1 SEMS ORGANIZATIONAL LEVELS

SEMS consists of five organizational levels:

1. **Field Response Level:** Commands emergency response personnel and resources to carry out tactical decisions and activities in direct response to an incident or threat
2. **Local Government Level:** Manages and coordinates a jurisdiction's overall emergency response and recovery activities
3. **Operational Area (OA) Level:** Manages and coordinates information, resources, and priorities among local governments within the San Bernardino County OA and serves as the coordination and communications link between the local and regional levels
4. **Regional Level:** Manages and coordinates information and resources among OAs within a mutual aid or administrative region (designated pursuant to

California Government Code § 8600) and between the OAs and the State. The regional and State levels coordinate overall State support for emergency response and recovery activities

5. **State Level:** Manages State resources in response to the emergency needs of the other levels, manages and coordinates mutual aid among the mutual aid regions and between the regional and State levels, and serves as the coordination and communication link with the Federal disaster support system

3.3.2 SEMS ORGANIZATIONAL FUNCTIONS

SEMS organizes the EOC into five primary functions:

- **Management Function:** Responsible for overall emergency policy and coordination through joint efforts of governmental agencies and private organizations
- **Operations Function:** Responsible for coordinating jurisdictional operations to support the emergency by implementing the action plan
- **Planning & Intelligence Function:** Responsible for collecting, evaluating, and disseminating information; developing the action plan in coordination with other functions; and maintaining incident records and documentation
- **Logistics Function:** Responsible for providing facilities, services, personnel, equipment, and materials to support incident response
- **Finance & Administration Function:** Responsible for all incident financial activities and administrative aspects not assigned to the other functions

3.3.3 IMPLEMENTING SEMS

SEMS will be used when the City EOC is activated or when a Local Emergency, as defined in California Government Code § 8558(c), is proclaimed. When the EOC is activated, communications and coordination will be established between the Incident Commander (IC) and EOC.

Communications and coordination will be established between the City EOC and any local and State response agencies having jurisdiction on an incident occurring within City boundaries. As defined in California Government Code § 8607(a), the City will use multi-agency coordination to facilitate decisions for City-level emergency response activities.

3.4 NATIONAL INCIDENT MANAGEMENT SYSTEM

The City has fully adopted the National Incident Management System (NIMS), as established by Homeland Security Presidential Directive-5 (HSPD-5), which integrates best practices into a consistent, flexible, and adjustable nationwide approach for emergency management.

Using NIMS, Federal, State, local and tribal governments, as well as private sector and non-governmental organizations work together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. Federal and State government agencies are required to use NIMS, while local government agencies and special districts must use NIMS to be eligible for Federal funding for emergency and disaster preparedness activities.

3.5 INCIDENT COMMAND SYSTEM

The Incident Command System (ICS)—which is part of both SEMS and NIMS—is a standardized, on-scene, all-hazards incident management approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private
- Establishes common processes for planning and managing resources

ICS is used in all levels of government and many non-governmental organizations and the private sector. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. ICS is also applicable across disciplines.

ICS is structured to facilitate activities in five major functional areas:

- **Command:** Responsible for directing response activities, including developing strategies, managing resources, and planning overall operations
- **Operations:** Responsible for coordinating the incident's tactical response and resources and for accomplishing incident-specific objectives
- **Planning:** Responsible for ongoing situation assessment; collection, evaluation, dissemination, and use of incident or event information; and

managing incident intelligence, including the status of response efforts and incident resources, to assist in the development of contingency plans

- **Logistics:** Responsible for providing facilities, services, and materials, including transportation and fuel, shelter, personal hygiene, food, potable water, tools, medical attention and supplies, communications, and relief personnel
- **Finance & Administration:** Responsible for tracking incident costs and evaluating the financial considerations of the incident

3.6 EMERGENCY SUPPORT FUNCTIONS

The City utilizes SEMS as required by California Government Code § 8607(a), structuring emergency management into the five key functions.

San Bernardino County, the State of California, and the Federal government incorporate the Emergency Support Function (ESF) model for providing emergency support during EOC activations. ESFs are designed to bring together discipline-specific stakeholders at all levels of government to collaborate and function within the five phases of emergency management.

Although the City does not use the Emergency Support Function (ESF) model, **Appendix F: ESF Crosswalk** of this EOP provides a crosswalk of ESFs to support coordination with San Bernardino County, Cal OES, and FEMA.

3.7 EMERGENCY PROCLAMATIONS

3.7.1 LOCAL EMERGENCY

A Local Emergency may be proclaimed by City Council or the Director of Emergency Services (MC § 2.52.100). A Local Emergency proclamation by the Director of Emergency Services must be ratified by City Council within seven days. City Council must review the need to continue the proclamation at least every 60 days until it terminates the Local Emergency. The Local Emergency may be terminated by resolution when conditions warrant. Proclamations are normally made when there is an actual incident, threat of disaster, or extreme peril to the safety of people and property within the City caused by natural or man-made situations. The proclamation of a Local Emergency provides the City with legal authority to:

- Request that the Governor proclaim a State of Emergency

- Promulgate or suspend orders and regulations necessary to provide for the protection of life and property, including issuing orders or regulations imposing a curfew within designated boundaries
- Exercise full power to provide mutual aid to any affected area in accordance with local ordinances, resolutions, emergency plans, or agreements
- Request mutual aid support from the County and other jurisdictions
- Require the emergency services of any local official or employee
- Request necessary personnel and materials from any local department or agency
- Obtain vital supplies and equipment and, if required, immediately commandeer the same for public use
- Impose penalties for violation of lawful orders
- Conduct emergency operations without incurring legal liability for performance or failure of performance (see Article 17 of the Emergency Services Act for privileges/immunities)

3.7.2 STATE OF EMERGENCY

A State of Emergency may be proclaimed by the Governor when:

- Conditions of disaster or extreme peril exist which threaten the safety of persons and property within the State caused by natural or man-made incidents
- The Governor is requested to do so by local authorities
- The Governor finds that local authority is inadequate to cope with the emergency

When a State of Emergency has been proclaimed:

- The Governor shall, to the extent deemed necessary, have the right to exercise all police power vested in the State by the Constitution and the laws of the State within the designated area
- Jurisdictions may command the aid of citizens as deemed necessary to cope with an emergency

- The Governor may suspend the provisions of orders, rules or regulations of any State agency and any regulatory statute or statute prescribing the procedure for conducting State business
- The Governor may commandeer or make use of any private property or personnel (other than the media) in carrying out the responsibilities of their office
- The Governor may promulgate, issue, and enforce orders and regulations deemed necessary

3.7.3 STATE OF WAR EMERGENCY

Whenever the Governor proclaims a State of War Emergency, or if a State of War Emergency exists, all provisions associated with a State of Emergency apply, additionally:

- All State agencies and political subdivisions are required to comply with the lawful orders and regulations of the Governor which are made or given within the limits of his authority as provided for in the Emergency Services Act.

3.8 OPERATING CONDITIONS

Operating Conditions have been established to provide a general indicator of the level of seriousness of an incident, impending incident, and current or anticipated emergency conditions. Operating Conditions and related guidance for lead and support departments will guide the readiness and response actions necessary to handle actual or impending emergencies. Operating Conditions do not reflect EOC Activation Levels, which are described in **Section 3.10: EOC Activation Levels** of this EOP. Operating Conditions are provided in Table 3.8 below.

Table 3.8 – Operating Conditions

OPERATING CONDITIONS		
Level	**Description**	**Associated EOC Activation Level**
Green	Normal Operations	None
Yellow	Increased Readiness	Management Watch
Red	Emergency Operations	Level 3, 2, 1

3.8.1 NORMAL OPERATIONS

GREEN: Under Normal Operations, departments conduct planning, training, and exercise activities to fulfill their roles in the EOP. They are staffed and operate per normal business operations, while also preparing for the next operating condition.

This condition is not associated with any EOC Activation Level.

3.8.2 INCREASED READINESS

YELLOW: Under Increased Readiness, events or conditions pose an actual or potential threat to life and property in threatened areas. Departments are taking increased readiness activities before an impending or potential emergency. Department Operations Centers (DOCs) may be activated to facilitate information and resource management. Agencies, departments, and special districts should prepare for the next operating condition.

This condition may be associated with Management Watch.

3.8.3 EMERGENCY OPERATIONS

RED: During Emergency Operations, events significantly impact life and property in affected areas. The EOC is activated and staffed, with DOCs activated as needed. Departments are taking all appropriate response actions, including curtailing non-essential operations and implementing special staffing patterns. This status is maintained until conditions de-escalate. Agencies, departments, and special districts should prepare for sustained emergency operations.

This condition may be associated with EOC Activation Levels 3, 2 or 1.

3.8.4 NOTIFICATION AND MOBILIZATION OF RESPONSE FORCES

The following is the process for notifying and mobilizing response forces in the City of Redlands:

City of Redlands EOC Team:

- By the Emergency Management Specialist, Redlands Police Department Dispatch Center, or designated alternate. Notification will be made through the City's Rave alerting system (Rave) or email to text.

City of Redlands Police Department:

- By the Redlands Police Department Dispatch Center.

City of Redlands Fire Department:

- By the CONFIRE Communications Center or via the on-duty Battalion Chief.

City of Redlands Departments:

- By each Department Operations Center, on-call staff person, or department administrative center.

Mutual Aid:

- By the respective City department or Mutual Aid Coordinator. Mutual aid resources are managed consistent with Section 8: Mutual Aid and Resource Management of this plan.

3.9 EOC ACTIVATION AND DEACTIVATION

3.9.1 EOC ACTIVATION

The EOC will become activated:

- By order of the City Manager as the Director of Emergency Services designated under MC § 2.52.080, or the Assistant City Manager(s) as Assistant Director(s) of Emergency Services, or the Fire Chief as the Emergency Manager, or a designee, or
- Upon the proclamation of a local emergency or when conditions exist that may warrant such a proclamation, consistent with the authority granted in MC § 2.52.100, or
- When the Governor has proclaimed a State of Emergency in an area, including the City of Redlands, or
- At the proclamation of a State of War Emergency, as defined by the California Emergency Services Act, or
- Upon a Triggering Event identified within this section.

3.9.2 TRIGGERING EVENTS

The following events may trigger the activation of the EOC:

- Damaging earthquake, wildfire, flood, or other impactful event
- Severe weather warning
- Significant commitment or draw-down of City emergency resources

- Regularly scheduled emergency exercises or training activities
- City special or planned events of significance
- Any incident that inhibits the City's ability to deliver essential services
- Any situation that requires coordinated, multi-department action through the EOC to protect life, property, or public safety

3.9.3 EOC SETUP AND STAFFING

Notification will be made to the Fire Chief as the Emergency Manager (or designee), who will oversee and coordinate the EOC's physical activation, setup, and staffing. The Fire Chief as the Emergency Manager (or designee) is responsible for maintaining the readiness of the EOC.

3.9.4 EOC NOTIFICATION AND MOBILIZATION

Notification of an EOC activation will be initiated by the City Manager, Assistant City Manager, Fire Chief, or their designee**.** Upon direction to activate, the Emergency Management Specialist, Police Communications Center, or the Duty Fire Battalion Chief will carry out the notification using the City's RAVE Alerting System, supplemented as needed by telephone, text message, or email using established City contact lists and pre-identified EOC staffing rosters.

Notifications regarding impending or actual emergencies may originate from the Redlands Police Department Communications Unit, Redlands Fire Department, CONFIRE Communications Center, San Bernardino County Sheriff's Department, San Bernardino County Office of Emergency Services (OES), National Weather Service, or a utility provider.

3.9.5 NOTIFICATION TO THE OPERATIONAL AREA

The San Bernardino County OES will be notified of a City EOC activation as soon as practical. The responsibility for making this notification lies with the Director of Emergency Services/EOC Director, the EOC Manager/Coordinator, or a designee. The County will subsequently be notified when the EOC is deactivated.

3.9.6 ACTIVATION OF THE ALTERNATE EOC

The Alternate City EOC will be activated whenever the Primary City EOC is uninhabitable, inaccessible, or located in a high-hazard zone due to an emergency.

3.9.7 EOC DEACTIVATION

The Director of Emergency Services/EOC Director or Assistant Director(s) of Emergency Services will direct the deactivation of the EOC when conditions no longer require its operation. As the situation deescalates, the EOC will be deactivated, and all positions and functions will be demobilized.

3.10 EOC ACTIVATION LEVELS

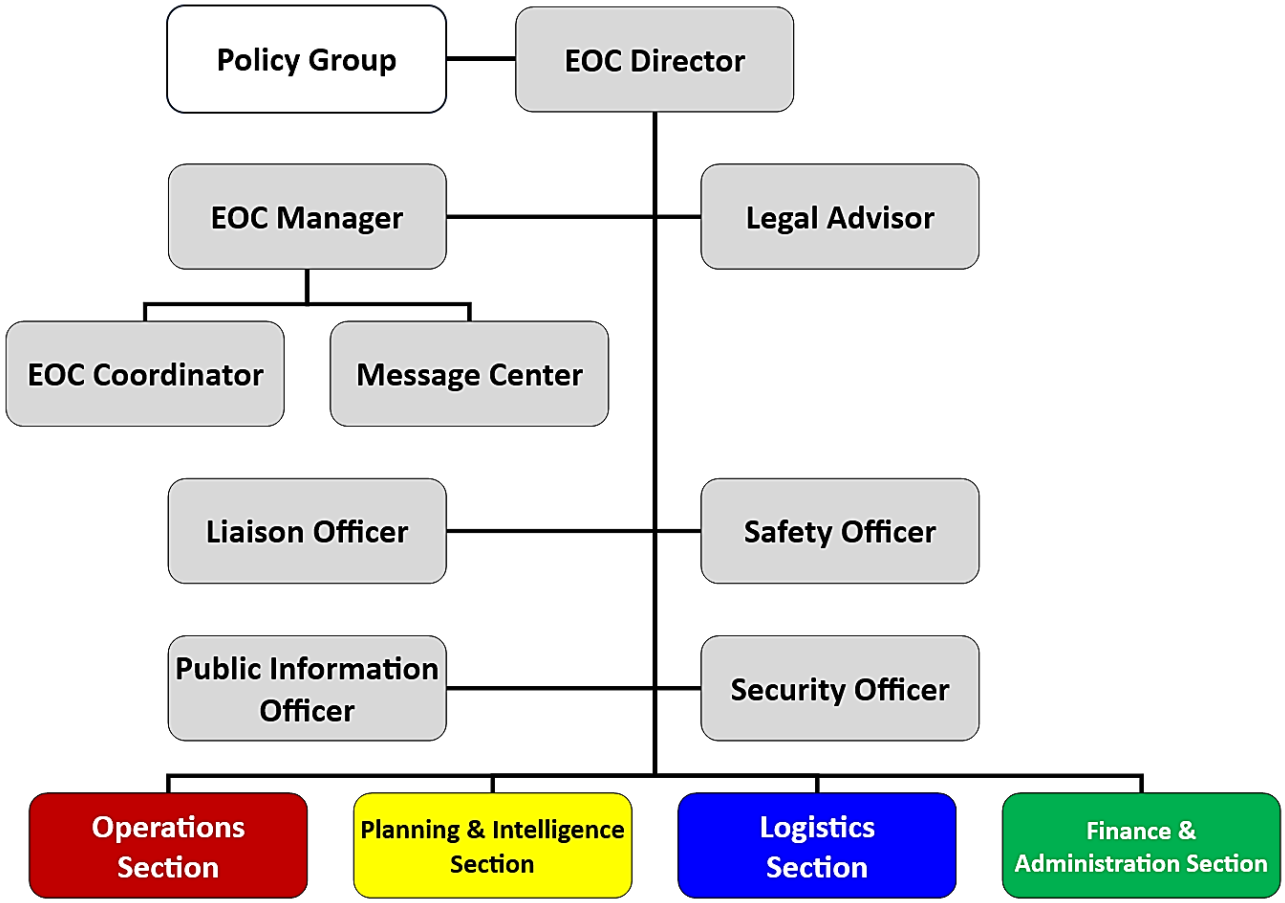
EOC activation levels are used to describe the scale and severity of an incident, the extent of coordination required, and the degree of support required from City departments and other agencies.

3.10.1 LEVEL 3: MINIMAL STAFFING

Impending or actual emergencies have prompted an increase in activity at the EOC. Essential EOC functions are activated, commensurate to the impending or actual emergency.

Level 3 staffing may include the Management Section, Section Chiefs, and any required support personnel. Other EOC Team members may be required to be readily available by phone. Level 3 staffing is illustrated in Graphic 3.10.1 on the next page.

Graphic 3.10.1 – Level 3 Staffing

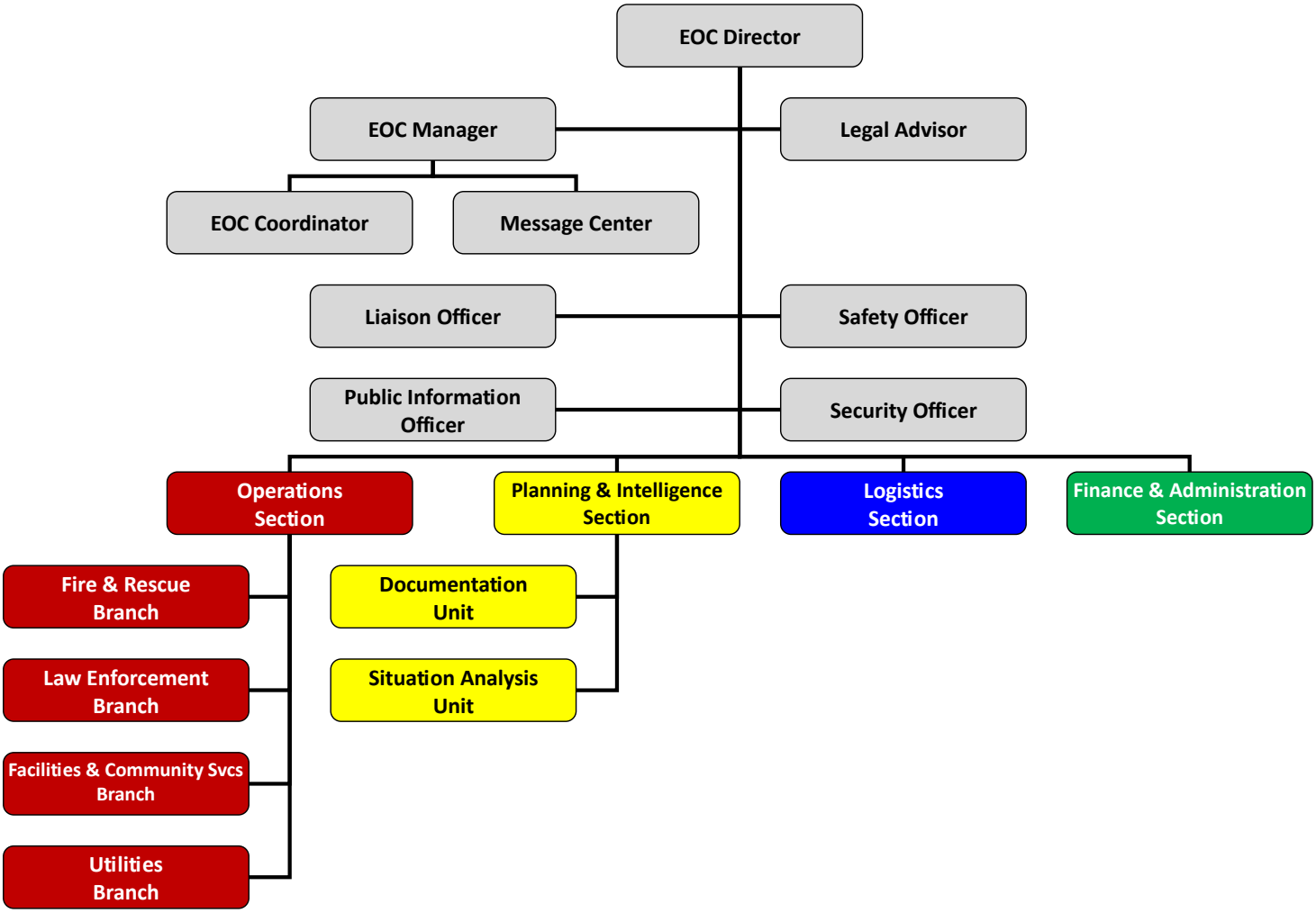


3.10.2 LEVEL 2: PARTIAL STAFFING

Impending or actual emergencies have prompted an increase in activity at the EOC. Essential EOC functions are activated, commensurate to the impending or actual emergency.

Level 2 staffing may include the Management Section, Section Chiefs, Branch Directors, and any required support personnel. Other EOC Team members may be required to be readily available by phone. Level 2 staffing is illustrated in Graphic 3.10.2 below.

Graphic 3.10.2 – Level 2 Staffing

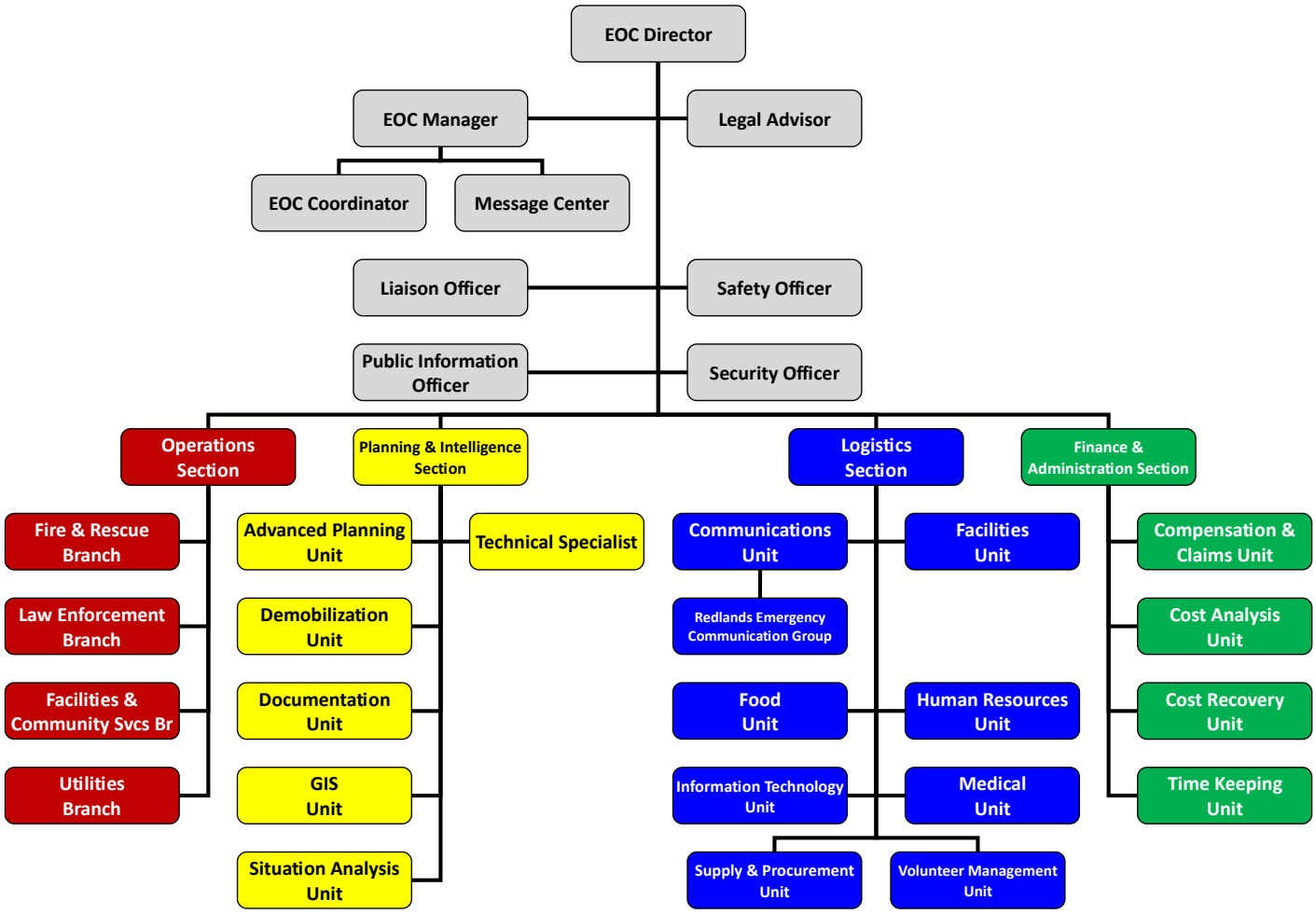


3.10.3 LEVEL 1: FULL STAFFING

Actual emergencies have prompted the full and complete activation of the City EOC. Essential EOC functions are activated commensurate to the emergency.

Level 1 staffing may include the Management Section, Section Chiefs, Branch Directors, Unit Leaders, and all required support personnel. Level 1 staffing will generally include all EOC functions and positions. Other EOC Team members may be required to be readily available by phone. Level 1 staffing is illustrated in Graphic 3.10.3 below.

Graphic 3.10.3 – Level 1 Staffing



3.10.4 MANAGEMENT WATCH

City departments or management staff may be required to monitor an evolving or potential emergency incident without activation of the EOC. This is referred to as a

Management Watch and involves close situational monitoring conducted outside of the EOC. A Management Watch does not constitute an EOC activation level.

3.11 EOC STAFFING MATRIX FOR CITY DEPARTMENTS

Each EOC function is assigned to one or more City departments. Department EOC assignments are found in **Appendix E: EOC Staffing Matrix for Departments** of this EOP.

3.12 EOC ACTION PLANS

At local, OA, regional and State levels, the use of EOC Action Plans provide designated personnel with knowledge of the objectives to be achieved and the steps required for achievement. EOC Action Plans not only provide direction, but they also serve to provide a basis for measuring achievement of objectives and overall system performance.

EOC action planning is an important management tool that involves:

- A process for identifying priorities and objectives for response or recovery efforts
- Documentation of the priorities, objectives, tasks, and personnel assignments

The action planning process should involve Management and General Staff along with other EOC elements, special district representatives, and other agency representatives as appropriate. The Planning & Intelligence Section is normally responsible for the development of the EOC Action Plan and the facilitation of action planning meetings.

EOC Action Plans are developed for a specified operational period that may range from a few hours to 24 hours. The operational period is determined by first establishing a set of priority actions that need to be performed. A reasonable time frame is then established for accomplishing those actions. EOC Action Plans need not be complex but should be sufficiently detailed to guide EOC elements in implementing the priority actions.

An EOC Action Plan is strategic and therefore not meant to replace a field-based Incident Action Plan (IAP). The EOC Action Plan should be coordinated with any existing IAPs.

3.13 CULTURAL COMPETENCE

Cultural competence is the ability to understand, respect, and appropriately respond to the diverse values, beliefs, and customs of different cultural groups. It is a critical component of equitable emergency preparedness, response, and recovery since disasters may disproportionately impact culturally diverse communities.

This EOP incorporates the requirements of California Government Code § 8593.3.5, which mandates consideration of cultural competence in all phases of emergency management. Key considerations include:

- Culturally and linguistically appropriate emergency communications, including the use of interpreters and translators
- Inclusive planning for evacuation and sheltering operations
- Culturally informed mitigation and prevention efforts
- Planning processes that engage qualified representatives from diverse community groups
- Preparedness education using culturally relevant outreach strategies and materials

The Director of Emergency Services/EOC Director will oversee implementation of these activities, with coordination handled by the appropriate EOC Sections and Branches.

3.14 DISABILITIES OR ACCESS AND FUNCTIONAL NEEDS POPULATIONS

Populations with disabilities or access and functional needs (DAFN) are community members who may require additional support before, during, and after an emergency in areas such as maintaining independence, communication, transportation, supervision, language, and medical care.

The City has identified its DAFN populations using the most recent US Census Bureau statistics:

- 15% of the population is 65 years and over
- 7.7% of the population is under 65 years and disabled
- 28.4% of the population speaks a language other than English at home

The EOP includes provisions to ensure that emergency notification, evacuation, transportation, and sheltering operations accommodate DAFN individuals. The City's planning efforts include:

- Notification and warning procedures, including Reverse 911
- TDD/TTY contact and captioned cable alerts for the hearing-impaired
- Accessibility of emergency information in multiple formats
- Language interpretation through staff skills and service contracts
- ADA-compliant access to facilities and shelters
- Transportation assistance for those requiring physical support
- Evacuation planning and emergency transportation coordination
- Accessibility for mobility devices, service animals, and medical needs (e.g., medications, refrigeration, backup power)

3.14.1 REQUIREMENTS OF THE AMERICANS WITH DISABILITIES ACT

Access to emergency services shall not be denied on the basis of race, color, national origin, sex, age, or disability. The City will ensure that all phases of emergency management address the needs of individuals protected under the Americans with Disabilities Act (ADA).

Pursuant to ADA Title II Regulations, State and local governments must ensure that programs, services, and activities are accessible to people with disabilities. This obligation extends to:

- Physical accessibility of facilities, programs, services, and events
- Policy modifications necessary to provide equal opportunity for participation
- Effective communication to ensure individuals with DAFN can receive, understand, and act upon information during all phases of an incident

3.15 ANIMAL CARE CONSIDERATIONS

During EOC activations, animal care needs will be addressed by the Animal Services Division within the City's Facilities & Community Services Department.

3.15.1 PETS ACT

The Pets Evacuation and Transportation Standards Act of 2006 (PETS Act) directs that State and local emergency preparedness plans address the needs of people with pets and service animals after a major disaster, including the rescue, care, and sheltering of animals. The PETS Act amends the Stafford Act, and requires evacuation plans to consider the needs of individuals with household pets and service animals, prior to, during, and after a major disaster or emergency.

3.15.2 CALIFORNIA ASSEMBLY BILL 781

California Assembly Bill 781, which created California Government Code § 8593.10, mandates that cities update their emergency plans to designate at least one emergency shelter capable of accommodating individuals with pets upon the next revision of their plans.

The City maintains one emergency shelter that is compliant with California Assembly Bill 781 and has a Memorandum of Understanding (MOU) with a facility capable of sheltering larger animals. These shelters are identified in **Annex 3: Response Plan (2022)** of this EOP.

3.16 RECOVERY ORGANIZATION

City recovery operations will be managed by the Director of Emergency Services/EOC Director until a Recovery Manager is appointed, who will report to the Director unless otherwise designated.

Until a dedicated Recovery Organization is established, the EOC or its components will fulfill recovery functions. Coordination may involve City departments, community-based organizations, businesses, utilities, non-governmental organizations (NGOs), San Bernardino County departments, OA partners, the Joint Field Office (JFO), and FEMA.

3.17 RECOVERY OPERATIONS

The recovery phase of an emergency or disaster is often defined as restoring a community to its pre-disaster conditions. In other words, recovery refers to the actions taken by the City following a disaster to restore normalcy. Effective recovery consists of an array of interdependent and coordinated actions. The specific approach to recovery operations following a disaster will be determined by the location, type, magnitude, and effects of the incident. Recovery operations are

divided into three phases: short-term, mid-term, and long-term. All phases will be coordinated by the City EOC.

The City maintains a separate **Disaster Recovery Plan (2024)**.

3.17.1 SHORT-TERM RECOVERY

Short-term recovery refers to the measures taken by the City following a disaster. It addresses the health and safety needs beyond rescue, the assessment of the scope of damages and needs, the restoration of basic infrastructure, and the mobilization of the National Disaster Recovery Framework organizations and resources. This includes restarting and/or restoring essential services for recovery decision-making. Effective recovery consists of a complex array of interdependent and coordinated actions.

The goal of short-term recovery is to restore City services to at least minimal capacity operations. Short-term recovery includes:

- Assessment of the extent and severity of damages to homes and other property
- Restoration of services generally available in communities, such as water, food, and medical assistance
- Professional counseling when the sudden changes resulting from the emergency have resulted in mental anguish and inability to cope
- Utility and infrastructure restoration
- Expanded social, medical, and behavioral health services
- Re-establishment of City government operations
- Transportation route restoration
- Debris removal and clean-up operations
- Abatement and demolition of hazardous structures

3.17.2 MID-TERM RECOVERY

Mid-term recovery efforts will prioritize the restoration of community lifelines and essential services, reestablishing access to food and fuel, and transitioning mass care operations into other forms of assistance. Mid-term recovery includes:

- Survivor care including housing, medical, emotional, behavioral, legal, and financial support
- Survivor reunification to reunite displaced persons with family networks
- Restoring community lifelines, including safety and security; food, water, and shelter; health and medical; energy (power and fuel); communication, transportation, and hazardous materials
- Debris management on public and private property
- Damage and safety inspection of homes, businesses, schools, and infrastructure

3.17.3 LONG-TERM RECOVERY

Long-term recovery consists of actions that will return City functions back to normal pre-disaster levels of service. It is critical that the documentation functions during response continue and expand into long-term recovery. The major objectives of long-term recovery operations include:

- Coordination of delivery of long-term social and health services
- Re-establishment of the local economy to pre-disaster levels
- Recovery of disaster response costs
- Integration of hazard mitigation strategies into recovery planning and operations

Failure to strictly account for damage documentation and personnel costs can result in loss of reimbursement.

3.17.4 FINANCIAL COST RECOVERY

In the months and years following a disaster, cost recovery will be focused on making individuals, businesses, and governments "whole" again. Financial cost recovery activities may include:

- Connecting survivors with Individual Assistance (IA) programs
- Connecting businesses and industries with financial assistance, including disaster loans from the Small Business Administration
- Restoring government entities through Public Assistance (PA) programs and Fire Management Assistance Grants for wildfire recovery

3.17.5 DAMAGE ASSESSMENT

In the initial hours following a disaster, it is critical that the City conduct a Rapid Needs Assessment (RNA), which collects data to estimate the extent of the damage. The EOC Planning & Intelligence Section, in coordination with the Operations Section and Finance & Administration Section, will organize damage reporting. The Finance & Administration Section will calculate cost and cost-recovery reporting. The City will submit its damage reports to the San Bernardino County OA, likely through an online portal or via email.

Within several days of the disaster, the City will coordinate with San Bernardino County and the State to conduct an Initial Damage Assessment (IDA), which captures damage information and impacts that may influence eligibility for State or Federal support or assistance. Following the IDA, the State will verify the data to ensure the level of damage caused by the disaster rises to the level of State or Federal support eligibility and meets the required indicators.

If the IDA indicates that the disaster is eligible for Federal support, then the State will request a Joint Preliminary Damage Assessment (JPDA) from the Federal government. Once the FEMA Regional Office reviews the State request for a JPDA and validates the IDA information, the JPDA Team—consisting of local and State governments in coordination with FEMA and the Small Business Administration (SBA)—will conduct site visits and assess damages, compile cost estimates and documentation, and assess damage assessment information to support a major disaster declaration request.

3.17.6 DISASTER ASSISTANCE

Federal disaster assistance is divided into two forms: Individual and Public Assistance. Individual Assistance is provided by FEMA to individuals and families who have sustained losses due to disasters. Public Assistance can fund the repair, restoration, reconstruction, and replacement of a public facility or infrastructure damaged or destroyed by a disaster. The Federal government also offers non-Stafford Act disaster relief programs.

State disaster assistance may be available through the California Disaster Assistance Act (CDAA).

Recovery plans should address all types of assistance, methods of acquiring help, restrictions, and other pertinent information.

3.17.6.1 INDIVIDUAL ASSISTANCE

Individual Assistance (IA) consists of the following services provided to individuals and families:

- **Disaster Housing Assistance Program:** Provides temporary housing to disaster victims during presidentially declared disasters. This Federal program is administered by FEMA.
- **Disaster Mortgage and Rental Assistance Program:** Provides grants for home-related mortgage or rent payments to disaster victims, who because of a disaster have lost their job or business and face foreclosure or eviction from their homes. This Federal program is available under a presidentially declared disaster.
- **Housing and Urban Development (HUD) Program:** Offered to families that meet certain income guidelines and may provide a percentage of the rental cost for a limited period to disaster victims. This program is available under a presidentially declared disaster.
- **Small Business Administration (SBA):** Provides low interest loans to businesses and individuals who have suffered disaster losses. This program is automatically implemented following a presidential disaster declaration for Individual Assistance or may be implemented at the request of the Governor.
- **Individual and Family Grant Program (IFGP):** Provides grants to disaster victims who are not eligible for SBA loans. This program is available under a presidentially declared disaster.
- **Cora Brown Fund:** Provides disaster victims with assistance, provided they are not eligible for any other disaster assistance award from the government or other organizations. This program is available under a presidentially declared disaster.

3.17.6.2 PUBLIC ASSISTANCE

Public Assistance (PA) consists of various programs of disaster relief to the public and private nonprofit sectors:

- Debris Management
- Private Nonprofit Program (PNP)

- Safety Assessment Program (SAP)
- Technical Assistance Programs (TAP)
- Laws and Regulations

The public sector includes State and local government (City, County, special district). Private nonprofit includes certain eligible Private Nonprofits (PNP) or an Intermediary PNP applicant to receive State assistance for extraordinary costs incurred while aiding at the request of local agencies during a State disaster event.

FEMA processes PA grant funding according to the type of work the applicant undertakes. Eligible work is classified into Emergency Work and Permanent Work.

Emergency Work

- **Category A: Debris Clearance** – Clearance of debris, wreckage, demolition, and removal of buildings damaged beyond repair
- **Category B: Protective Measures** – Measures to eliminate or lessen immediate threats to life, public health, and safety

Permanent Work

- **Category C: Roads & Bridges** – All non-emergency work and any that may require more time for decision-making, preparation of detailed design, construction plans, cost estimates, and schedules
- **Category D: Water Control Facilities** – Includes flood control, drainage, levees, dams, dikes, irrigation works, and bulkheads
- **Category E: Public Buildings and Equipment** – Buildings, vehicles or other equipment, transportation systems, fire stations, supplies or inventory, higher education facilities, libraries, and schools
- **Category F: Utilities** – Water supply systems, sanitary sewage treatment plants, storm drainage, and light/power
- **Category G: Other** – Park facilities, public and private facilities, recreational facilities, and playground equipment

Federal funding guidelines for each of these categories are listed in the FEMA PA Program and Policy Guide, which can be found on the Cal OES website at https://www.caloes.ca.gov/wp-content/uploads/Recovery/Documents/FEMA-Public-Assistance-Policy-Guide-V4.pdf.

3.17.6.3 NON-STAFFORD ACT PROGRAMS

The Federal government provides recovery assistance through authorities and programs outside the Stafford Act. These programs may be implemented alongside Stafford Act programs under a disaster declaration. Depending on the program, the agencies assist recipients directly or through another State agency besides Cal OES. Examples include:

- **Federal Highway Administration (FHWA):** Under the Emergency Relief Program, the FHWA provides assistance to the Department of Transportation (Caltrans) and local governments for damage to roads, bridges, and other facilities on the Federal aid system. Caltrans implements this program on behalf of FHWA.
- **Natural Resources Conservation Service (NRCS):** Under the Emergency Watershed Protection Program, the NRCS provides assistance to State agencies and local governments for emergency work necessary to protect life, property, and public health and safety in watersheds damaged by a disaster, such as wildfire or flood.
- **U.S. Army Corps of Engineers (USACE):** Under the Rehabilitation and Inspection Program, the USACE assists in flood fighting, emergency repairs, and repairs to damaged facilities. The USACE provides this assistance for levees and other flood control works that meet pre-disaster program participation criteria.
- **U.S. Department of Housing and Urban Development (HUD):** HUD Community Development Block Grants may be requested by State and local governments for a wide range of recovery purposes.
- **Congressional Appropriations:** Congress may make disaster-specific appropriations that allow Federal agencies to provide assistance beyond existing authorities and programs. State coordination of this assistance depends on the nature of the appropriation and the Federal agency charged with its implementation.

3.17.6.4 CALIFORNIA DISASTER ASSISTANCE ACT

The California Disaster Assistance Act (CDAA) provides State financial assistance for recovery efforts to cities, counties, special districts, and certain eligible private nonprofit agencies after a Cal OES Director's Concurrence or the Governor's

Proclamation. CDAA may be implemented as a "standalone" funding source following a State disaster.

CDAA is available to cities, counties, and special districts to repair disaster-related damage to public buildings, levees, flood control works, channels, irrigation works, City streets, County roads, bridges, and other public works except those facilities used solely for recreational purposes. This program offers a percentage of the eligible cost to repair, restore, reconstruct or replace public property or facilities; to cover direct and indirect costs of grant administration with the Cal OES Director's concurrence; and to cover the cost of overtime and supplies used for response. The conditions for implementation of the CDAA are as follows:

- The Cal OES Director must concur with a local emergency declaration for permanent restoration assistance
- The Governor must proclaim a State of Emergency for disaster response and permanent restoration assistance
- The President must declare a major disaster or emergency for matching fund assistance for cost sharing required under Federal public assistance programs

Note: Local proclamations of emergency should, when known at the time of issuance, specify any requests being made to the State, including anticipated needs for California Disaster Assistance Act (CDAA) assistance.

3.17.7 NON-GOVERNMENTAL ORGANIZATIONS AND COMMUNITY BASED ORGANIZATIONS

Non-Governmental Organizations (NGOs) and Community-Based Organizations (CBOs), such as the American Red Cross and the Salvation Army, typically provide support to individuals and households who are displaced by a disaster and work with governmental organizations to support the transition from care and shelter operations to interim housing arrangements. Community organizations active before a disaster may expand their services to meet increased needs. Such groups include faith-based organizations, neighborhood health clinics, and food distribution agencies. NGOs and CBOs may provide a range of services such as donations management, emergency food, clothing and shelter, behavioral and spiritual counseling, assist with non-hazardous debris removal from private

property, as well as support of housing reconstruction. They provide these services independently or in coordination with Federal, State, and local efforts.

3.17.8 RECOVERY REPORTING AND DOCUMENTATION

Recovery reporting and documentation is the key to recovering eligible emergency response and recovery costs. Damage assessment documentation will be critical in establishing the basis for eligibility of disaster assistance programs. Without proper documentation, the County and local jurisdictions may be liable to FEMA for disaster recovery funding.

3.17.8.1 RECOVERY DOCUMENTATION

Recovery documentation information should include the location and extent of damage, and estimates of costs for debris removal, emergency work, and repairing or replacing damaged facilities to a non-vulnerable and mitigated condition. The cost of compliance with building codes for new construction, repair, and restoration will also be documented. The cost of improving facilities may be provided under Federal hazard mitigation grant programs. Documentation is the key to recovering expenditures related to emergency response and recovery operations. Documentation must begin at the field response level and continue as the disaster unfolds. The EOC Planning & Intelligence Section, in coordination with the Operations Section and Finance & Administration Section, organizes damage reporting.

3.17.8.2 AFTER-ACTION REPORTING

The California Code of Regulations § 2450(a) requires the submission of After-Action Reports to Cal OES within 90 days of the close of an incident period for locally declared emergencies for which the Governor proclaims a State of Emergency.

An After-Action Report serves the following important functions:

- Provides a source for documenting response and early recovery activities
- Identifies problems and successes during emergency operations
- Analyzes the effectiveness of the different components of SEMS
- Identifies, documents, and facilitates corrective action for implementing and tracking improvements to existing emergency response and recovery efforts

The Fire Chief as the Emergency Manager (or designee) is responsible for coordinating the After-Action Review process and ensuring the After-Action Report is submitted.

3.17.9 JOINT FIELD OFFICE

Following a Presidential Declaration of a Major Disaster or Emergency, a Joint Field Office (JFO) will be established in proximity to the disaster area. The JFO is the direction and coordination point for Federal assistance. The State will appoint a State Coordinating Officer (SCO) to serve as the State point of contact. A Federal Coordinating Officer (FCO) is appointed upon a Presidential Declaration of an Emergency or Major Disaster.

3.17.10 COMMUNITY LIFELINES

FEMA defines Community Lifelines as those services or systems that "enable the continuous operation of critical government and business functions and is essential to human health and safety or economic security."

Stabilizing lifeline services is the top priority in disaster response due to immediate threats to life and property. Community Lifeline descriptions help responders assess conditions and determine necessary recovery actions. The City EOC prioritizes lifeline restoration in its EOC Action Plan. Since many lifelines are managed externally, close coordination with utility providers and external organizations will be essential.

Graphic 3.17.10 – Community Lifelines

Source: FEMA

3.18 EMERGENCY FACILITIES

Emergency facilities supporting emergency operations are identified and described below.

3.18.1 PUBLIC SAFETY COMMUNICATIONS CENTERS

City calls for police, fire, and emergency medical services are dispatched from the following locations:

- Redlands Police Department Communications Unit

  1270 W. Park Ave, Redlands, CA 92373

- CONFIRE Communications Center

  1743 Miro Way, Rialto, CA 92376

3.18.2 DEPARTMENT OPERATIONS CENTERS

A Department Operations Center (DOC) is a coordination hub for specific disciplines—such as fire, police, public works, or utilities—to manage field-level emergency responses and support the EOC.

The City maintains the following DOCs:

- Police Department – Watch Commander's Office
- Fire Department – Duty Battalion Chief's Office
- Municipal Utilities & Engineering Department

3.18.3 PRIMARY/ALTERNATE EMERGENCY OPERATIONS CENTERS

The EOC is the location where centralized emergency management during large-scale emergencies and disasters takes place. The primary and alternate EOCs are provided in Table 3.18.3 below.

Table 3.18.3 – City Emergency Operations Centers

City Emergency Operations Centers	
Primary EOC	**Redlands Police Department** 1270 W. Park Ave, Redlands, CA 92373
Alternate EOC	**Redlands Wastewater Treatment Facility** 1950 Nevada St, Redlands, CA 92373

During EOC activations, the EOC Policy Group will meet at a location separate from the primary and alternate EOCs.

3.18.4 JOINT INFORMATION CENTER

The Joint Information Center (JIC) is a location where staff from various organizations with public information responsibilities can co-locate to perform critical emergency public information, crisis communications, and public affairs functions. The JIC for the City would be co-located with the EOC if needed.

3.18.5 INCIDENT COMMAND POST

The Incident Command Post (ICP) is the field location for primary tactical-level, on-scene incident command and management. It typically includes the Incident Commander (IC) and Command Staff, as well as other incident management officials, responders, public agency representatives, private-sector representatives, and non-governmental organizations.

3.18.6 STAGING AREA

A staging area is a temporary holding location for assigned resources, established by the Incident Commander or Operations Section Chief. It allows for the positioning and accounting of resources not immediately needed for an operational task. These areas are used to temporarily position personnel, supplies, and equipment while awaiting an assignment.

3.18.7 MOBILIZATION CENTER

A mobilization center is an off-incident location where emergency personnel and equipment are temporarily positioned while awaiting assignment, release, or reassignment. Unlike a staging area, it is generally activated and managed by the EOC. Mobilization centers support significant emergencies and disasters, serving as hubs for mutual aid resources.

3.18.8 EVACUATION RECEPTION CENTER

An evacuation reception center temporarily accommodates people displaced from their home, school, or business. It provides a safe and comfortable space for disaster survivors to receive relief until the incident concludes, or they transition to a mass care center or shelter. These centers are established for short-duration incidents where overnight assistance or a shelter is unnecessary, or as a temporary solution while a fully operational shelter is being set up, which can take several hours.

3.18.9 SHELTER

A shelter provides temporary care for those displaced by emergencies, offering sleeping accommodation and minimal necessities. Unlike evacuation reception centers, shelters are equipped for overnight stays and may operate alongside evacuation reception centers. Evacuees are encouraged to bring essentials like blankets, toiletries, and snacks. Shelters require significant planning, logistics, staffing, medical and mental health support, and security.

The City has designated 19 facilities to potentially serve as emergency shelter sites for displaced persons, along with two separate facilities for emergency animal sheltering. These shelters are identified in **Annex 3: Response Plan (2022)** of this EOP.

4. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

All City departments and employees have a role during emergency response and recovery operations. City employees are also Disaster Service Workers, per California Government Code § 3100, and may be called into service during proclaimed or declared disasters.

The City's emergency operations and organizational structure are organized according to the concepts and principles of SEMS and NIMS.

4.1 CITY LEVEL

The City of Redlands Emergency Organization (MC § 2.52.140) consists of "all officers and employees of the City, together with those volunteer forces enrolled to aid them during an emergency, and all groups, organizations, and persons who may be in agreement or operation of law, including persons impressed into service," who are "charged with duties incident to the protection of life and property in the City during such emergency."

4.1.1 DIRECTOR OF EMERGENCY SERVICES

The City Manager is the Director of Emergency Services, having jurisdiction and full authority over the City's response and recovery to extraordinary emergencies and disasters. The Assistant City Manager or Assistant City Managers serve as Assistant Directors of Emergency Services. Alternates may be designated by the Director of Emergency Services.

4.1.2 CITY COUNCIL

City Council may promulgate orders and regulations necessary to protect life and property, including orders and regulations to impose curfews and stop price fixing. Members of the City Council will serve as liaisons to constituents regarding the City's disaster response and recovery efforts. They will also liaise with County, State, and Federal elected officials, as appropriate and necessary.

4.1.3 ELECTED OFFICIALS

Elected officials, including City Council members, play a non-operational support role during disasters. During an active disaster response, elected officials best serve the public by supporting—rather than directing—trained emergency personnel and EOC staff. Their role is non-operational, focused on maintaining public confidence

and enabling responders to stabilize the situation without interference. Strategic decisions by elected officials may follow once the incident is under control. The immediate priority remains rapid, coordinated action by emergency professionals.

4.1.4 DISASTER COUNCIL

The City of Redlands maintains a Disaster Council accredited by the State of California.

The City of Redlands Disaster Council Membership (MC § 2.52.050) consists of the Mayor (Chairperson); the City Manager/Director of Emergency Services (Vice-Chairperson); the Emergency Services Chief; "groups that support a strong team merging sectors of the community including elected officials, emergency management, first responders, volunteer services, major industry and commercial, healthcare and education"; and a Citizen Corps Council that "shall be created as a subgroup of the Disaster Council."

The City of Redlands Disaster Council powers and duties (MC § 2.52.060) state: "It shall be the duty of the City Disaster Council, and it is empowered, to develop and recommend for adoption by the City Council emergency and mutual aid plans and agreements."

The Disaster Council should meet at least once per year, upon call of the Chairperson, or upon call of the Vice-Chairperson (in the absence of the Chairperson).

4.1.5 EMERGENCY MANAGER

The Fire Chief, serving as the Emergency Manager, oversees the City's emergency management program, including preparedness, response, recovery, and mitigation activities. Responsibilities include maintaining the EOP, coordinating interagency training and exercises, and ensuring compliance with Federal and State emergency management standards. The position also manages public outreach, resource allocation, and continuity planning for critical City functions. The Emergency Manager serves as the primary liaison during disasters, facilitating communication between City departments, regional partners, and emergency services.

4.1.6 FIRST RESPONSE DEPARTMENTS

First response departments are operational entities tasked with responding to and recovering from emergencies and disasters.

In the City, first response departments include:

- Fire Department
- Police Department
- Facilities & Community Services Department

First response departments are responsible for developing policies, procedures, guidance, and resources to enable them to execute their responsibilities in the EOP.

4.1.7 DEPARTMENT OPERATIONS CENTER

A DOC is a coordination hub for specific disciplines—such as fire, police, public works, or utilities—to manage field-level emergency responses and support the EOC.

The City maintains the following DOCs:

- Police Department
- Fire Department
- Municipal Utilities & Engineering Department

4.1.8 EMERGENCY OPERATIONS CENTER

The EOC is a centralized location for coordinating emergency response activities. The City maintains primary and alternate EOCs, the locations of which are identified in **Section 3.18: Emergency Facilities** of this EOP.

4.1.9 EOC TEAM

The EOC Team is responsible for managing all aspects of EOC operations when activated. This team comprises City employees assigned to EOC functions, who provide strategic planning and direction from the EOC. Management Staff support the EOC Director, while General Staff handle SEMS functional aspects, and are led by Section Chiefs who report to the EOC Director.

4.1.10 EOC POLICY GROUP

The EOC Policy Group provides executive-level advice and subject-matter input to the Director of Emergency Services during an extraordinary emergency or disaster. The group helps shape interim policy considerations, identifies organizational impacts, and ensures that emergency regulations, proclamations, and orders are legally sound and operationally feasible. The Policy Group convenes as needed to

support the Director's decision-making and maintain alignment with City priorities and statutory requirements.

The Policy Group consists of the City Manager, Assistant City Manager(s), Mayor Pro Tem, Fire Chief, Police Chief, Finance Director, Human Resources Director, and the Facilities & Community Services Director. Together, these positions provide comprehensive executive coverage for legal authority, fiscal oversight, operational leadership, personnel and labor-relations considerations, and continuity of government.

The City Attorney (Legal Advisor) and City Clerk serve in a support role to the Policy Group, with the City Clerk responsible for documenting and recording all emergency orders and decisions made during Policy Group deliberations.

4.1.11 CITY DEPARTMENTS

City departments and divisions will ensure they can fulfill their emergency management responsibilities. They provide incident response and support, including staffing DOCs and the EOC Team using SEMS and NIMS principles. They conduct damage assessments, implement continuity and communication plans, establish programmatic operational strategies, and restore essential infrastructure and services.

4.1.12 DISASTER SERVICES WORKERS

According to California Government Code § 3101, a Disaster Service Worker (DSW) includes all public employees and all volunteers in any disaster council or emergency organization accredited by Cal OES. All City employees, full-time and part-time, are DSWs and may be called upon during emergencies and disasters. In an emergency, non-essential public employees may be released from their usual duties so that they can be reassigned to assist any agency or organization carrying out its emergency response duties. Employees acting as DSWs will be assigned duties within their scope of training, skill, and ability.

4.2 OPERATIONAL AREA LEVEL

California Government Code § 8559(b) defines an Operational Area (OA) as "an intermediate level of the State emergency services organization, consisting of a county and all political subdivisions within the county area." Political subdivisions include cities and special districts. An OA has an agreement in place that defines

roles and responsibilities, as well as jurisdictional authority in an emergency. The City is signatory to this agreement.

The San Bernardino County OES serves as the OA Coordinator for emergency management. OES is responsible for coordinating emergency response efforts across jurisdictions within the OA. It serves as the central hub for aligning information, resources, and priorities between local governments and regional authorities. OES facilitates multi-agency and inter-agency collaboration to support unified decision-making. Its role ensures cohesive, area-wide emergency management during incidents. When the emergency impacts OA jurisdictions, the designated OA Coordinator is responsible for ensuring direction, coordination and communication of policy decisions, resource needs, and priorities between OA jurisdictions and the State throughout the emergency (San Bernardino County EOP, 2025).

4.3 REGIONAL LEVEL

The regional level manages and coordinates information and resources among OAs. Cal OES has divided California into three administrative regions which are further divided into six mutual aid regions. The City is in the Southern Region and Mutual Aid Region VI, which includes the counties of Imperial, Inyo, Mono, Riverside, San Bernardino, and San Diego. The Cal OES Southern Region in Los Alamitos will support the San Bernardino County OA EOC.

4.4 STATE LEVEL

In response to emergency needs and requests from local governments and OAs, the State coordinates mutual aid across mutual aid regions and between regional and state levels while managing its own resources. The State also acts as the primary coordination and communication link between the State and the Federal levels.

4.5 FEDERAL LEVEL

The U.S. Department of Homeland Security (DHS) has designated FEMA to serve as the lead federal agency during disasters and national security emergencies. In a disaster, different federal agencies may be involved in the response and recovery operations. Federal disaster assistance is organized under the concept of Emergency Support Functions (ESFs) as defined in the National Response Framework (NRF). All contact with FEMA and other federal agencies is made

through the OAs during the response phase. During the recovery phase, there may be direct City contact with FEMA and other federal agencies.

4.6 EXTERNAL PARTNERS

4.6.1 NON-GOVERNMENTAL ORGANIZATIONS

Non-governmental organizations (NGOs) play essential roles before, during, and after disasters. NGOs provide a wide range of services such as shelter operations, donations management, food distribution, non-hazardous debris removal, and housing reconstruction support. They provide these services independently or in coordination with Federal, State, and local efforts.

American Red Cross (ARC): Humanitarian organization dedicated to providing emergency assistance, disaster relief, and education. Its core purpose is to help people in crisis by offering life-saving services, such as blood donation drives, disaster response, and supporting military families. The organization also focuses on disaster preparedness, health and safety education, and recovery efforts, aiming to alleviate human suffering and strengthen community resilience. For more information, go to:

https://www.redcross.org/local/california/southern-california.html

National Voluntary Organizations Active in Disaster (NVOAD): Coalition of nonprofit organizations in the U.S. that collaborate to provide disaster relief and recovery services. Its purpose is to coordinate efforts, share resources, and reduce duplication of services, ensuring an efficient and effective response to disasters. NVOAD focuses on providing immediate assistance, long-term recovery, and helping communities prepare for future disasters through member organizations' expertise and volunteer mobilization. For more information, go to:

https://www.nvoad.org

San Bernardino County Voluntary Organizations Active in Disaster (SBCOVOAD): Coalition of nonprofits, faith-based and community organizations, businesses, tribal partners, and government agencies working together to strengthen disaster preparedness, response, and recovery across the largest county in the nation. For more information, go to:

https://sbcovoad.org

Salvation Army: Humanitarian organization focused on providing emergency assistance, disaster relief, and social services to those in need. Its purpose is to alleviate human suffering, promote social justice, and offer hope through programs such as food distribution, shelter, addiction recovery, and disaster response. The Salvation Army works to meet both immediate and long-term needs, serving all individuals and communities. For more information, go to:

https://sanbernardino.salvationarmy.org/san_bernardino_corps

4.6.2 PRIVATE SECTOR

The private sector plays a vital role in the economy and provides essential goods and services that sustain daily life. The City has developed many public-private partnerships and relies on its private sector partners for disaster response and recovery.

According to DHS, the private sector owns and operates approximately 80% of the nation's critical infrastructure, such as energy, telecommunications, transportation, water and wastewater systems, chemical and manufacturing industries, healthcare, and insurance and financial services. The remaining 20% of critical infrastructure is managed by Federal, State, and local governments and typically includes emergency services, public transportation systems, and some water and sewage systems.

Private companies in sectors like food, transportation, healthcare, and logistics provide essential goods and services during and after a disaster. Many of these companies fill critical needs in the community through the donation of goods and resources, in addition to contributing funds to disaster relief and recovery efforts.

4.6.3 SCHOOLS AND ACADEMIC INSTITUTIONS

Schools and academic institutions can serve as centers for recovery, stability, and community support after a disaster, in addition to their traditional educational function. Following a disaster, schools contribute by:

- Serving as shelters for displaced individuals
- Serving as points of distribution for relief supplies
- Providing counseling and mental health services for students and their families
- Reestablishing normalcy for students following disasters

- Providing disaster preparedness training for students and their families

In California, K-12 public schools are required to have disaster plans, conduct periodic drills, and provide educational and training programs to staff and students. Schools and academic institutions should train students and staff in proper emergency response procedures and educate student families on school plans and procedures during and after an emergency (including student release procedures).

4.6.4 FAITH-BASED ORGANIZATIONS

Faith-based organizations (FBOs) play a critical role in all four phases of emergency management and should be incorporated into emergency planning and disaster response. FBOs provide various forms of aid following a disaster and often participate in long-term recovery efforts.

FBOs contribute by:

- Engaging with communities on topics such as household disaster preparedness, hazard mitigation, and basic medical care
- Providing shelter for displaced individuals
- Providing counseling and emotional/spiritual support
- Distributing food, water, and clothing to the community
- Collecting, managing, and distributing donations (cash and material)
- Mobilizing volunteers to assist with tasks such as evacuation, rescue, and basic medical care
- Collaborating with NGOs to ensure aid is distributed fairly and appropriately
- Advocating for the needs of marginalized and vulnerable populations
- Supporting long-term recovery efforts in the form of financial assistance, rehabilitation programs, community cohesion, and rebuilding homes

4.6.5 COMMUNITY INVOLVEMENT

Resilient communities begin with prepared communities. Individuals, families, and caregivers to those with access and functional needs should enhance their awareness of risks and threats, develop household emergency plans that include care for pets and service animals, and prepare emergency supply kits. Individuals can also volunteer in their communities.

Individuals and households play an essential role in emergency management by contributing to community, neighborhood, and family preparedness.

Community members can contribute by:

- Reducing hazards in and around their homes. Hazard reduction actions include making their home earthquake-resistant or storing unanchored objects during high winds. These actions can reduce damage caused by an emergency.
- Preparing an emergency supply kit and household emergency plan. By developing a household emergency plan and assembling disaster supplies before an emergency, people can take care of themselves until assistance arrives. Emergency kits should include supplies for household pets and service animals.
- Monitor emergency communications carefully. Critical information and directions will be released to the public via various media throughout an emergency. By carefully following the directions provided, residents can reduce their risk of injury, keep emergency routes open to response personnel, and reduce the demands on landline and cellular communication.
- Volunteering with an established organization such as CERT. Organizations and agencies with a role in response and recovery are always seeking hardworking and dedicated volunteers. By volunteering with an established volunteer agency, individuals and households become a part of the emergency management system and ensure that their efforts are directed where they are most needed.
- Enrolling in emergency response training courses. Emergency response training, whether basic first aid through the ARC or a more complex course through a local college, will enable residents to take initial response actions required to care for themselves and their households. This allows first responders to focus on higher-priority tasks that affect the entire community.

THIS PAGE IS INTENTIONALLY LEFT BLANK

5. DIRECTION, CONTROL, AND COORDINATION

Direction, control, and coordination define the organizations within the multi-agency coordination system, clarify their roles in emergency operations, and describe how coordination is achieved.

5.1 DIRECTOR OF EMERGENCY SERVICES

The City Manager serves as the Director of Emergency Services and holds full authority over the City's emergency response and recovery efforts. These powers are established in MC § 2.52.100 (Powers and Duties of the Director of Emergency Services).

5.2 CITY EOC

During an emergency or disaster, the City's emergency management functions will be conducted from the primary EOC, located at the Redlands Police Department (1270 W. Park Ave, Redlands, CA 92373). In addition to overseeing City response activities, the EOC serves as the primary link to the San Bernardino County OA and mutual aid partners.

5.3 CITY DEPARTMENT DIRECTION

Each City department operates under its Department Director or designated alternate in preparing for and responding to City emergencies and disasters. When the EOC is activated, department representatives coordinate emergency management functions from the EOC and are empowered to make decisions and allocate resources in accordance with the EOC Action Plan or as directed by the Director of Emergency Services/EOC Director.

5.4 DEPARTMENT OPERATIONS CENTERS

When activated, the management and coordination of department-level response and recovery activities for citywide events, extraordinary emergencies, and disasters will be directed from DOCs.

5.5 LOCAL CONTROL

Local governments manage emergency operations within their jurisdictions in compliance with applicable laws, orders, and regulations. When the City is the Authority Having Jurisdiction (AHJ), it oversees incidents from response to recovery. As outlined in the California Government Code § 8618, the City directs

mutual aid incidents, including personnel and equipment from mutual aid programs. Mutual aid resources remain under the operational control of their respective disciplines and designated Incident Commander (IC).

5.6 ON-SCENE CONTROL

An Incident Commander (IC) from an Incident Command Post (ICP) directs and controls on-scene tactical activities, supporting single incidents, countywide events, complex incidents, or when in an Area Command structure. This on-scene control includes setting tactical objectives and managing resources, including mutual-aid resources. The EOC and DOCs support rather than direct on-scene tactical activities.

5.7 COORDINATION AND INTERFACE

5.7.1 EOC-FIELD COORDINATION AND INTERFACE

EOC-to-field communications typically occur at the Command and General Staff levels and are relayed to the appropriate section or function within the EOC. For example, the Fire-Rescue Branch in the EOC generally communicates directly with the Fire Incident Commander during fire-related incidents.

To support EOC-field coordination and establish a common operating picture, the EOC may consider the following activities to facilitate communication and interface with field operations:

- Assign an EOC representative to the Incident Command Post (ICP)
- Have an EOC representative attend ICP operations briefings
- Have an ICP representative attend EOC operations briefings
- Coordinate and share EOC Action Plans with the ICP
- Coordinate and share ICP Incident Action Plans (IAPs) with the EOC
- Share EOC Situation Reports with the ICP
- Share ICP Situation Reports with the EOC

5.7.2 EOC-DOC-FIELD COORDINATION AND INTERFACE

Effective emergency response depends on coordination across all SEMS levels. In major incidents, the City EOC may activate to manage the broader response, while DOCs support field command posts when multiple incidents strain departmental

resources. Field ICs communicate with their respective DOCs or directly with the EOC Operations Section, based on the nature of the incident. DOCs maintain situational awareness and may activate independently to manage multiple incidents, under the direction of the Department Director. The City EOC facilitates communication with ICPs and DOCs as needed.

5.7.3 OPERATIONAL AREA COORDINATION

OA coordination is maintained through each jurisdiction's Emergency Manager, who serves as the primary link between local EOCs and the San Bernardino County OES, which operates the OA EOC. The OA supports countywide coordination by gathering and sharing situational information, facilitating resource requests, and maintaining consistent communication across jurisdictions. Member agencies use the Multiagency Coordination System to prioritize incidents and share resources, with situation reporting and resource coordination managed through the OA's WebEOC platform.

5.7.4 MULTIAGENCY COORDINATION

Multiagency coordination enables all levels of government to establish incident priorities and allocate resources across multiple incidents or jurisdictions. The Multiagency Coordination System (MACS) integrates personnel, procedures, and communication systems to support unified decision-making.

MAC Groups may include:

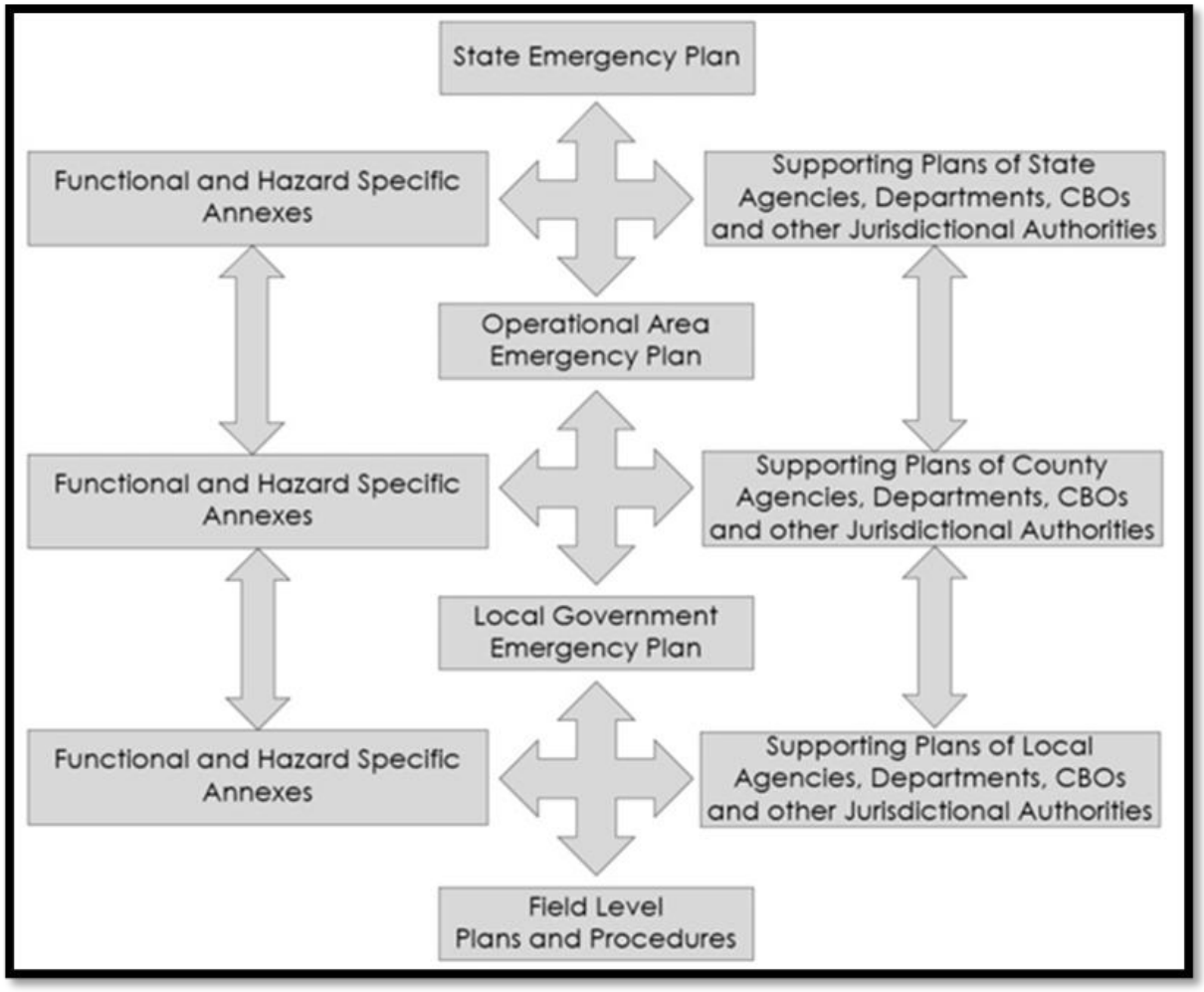
- Representatives from the City departments
- Representatives from outside agencies including special districts, volunteer agencies, and private partners
- Coordination with agencies not represented in the EOC
- Departments and agencies in the EOC action planning
- OA Mutual Aid Coordinators and mutual aid providers

The OA EOC may coordinate conference calls before or during emergencies. In this case, the OA jurisdictions may serve as a MACS Group to coordinate situational information and share resources. The City most often participates in a MAC System or Group through OA emergency management coordination.

5.7.5 EMERGENCY PLAN COORDINATION

The City EOP functions within a broader planning framework that supports emergency management at the local and regional levels. Graphic 5.7.5 below illustrates this coordinated framework.

Graphic 5.7.5: Emergency Plan Coordination

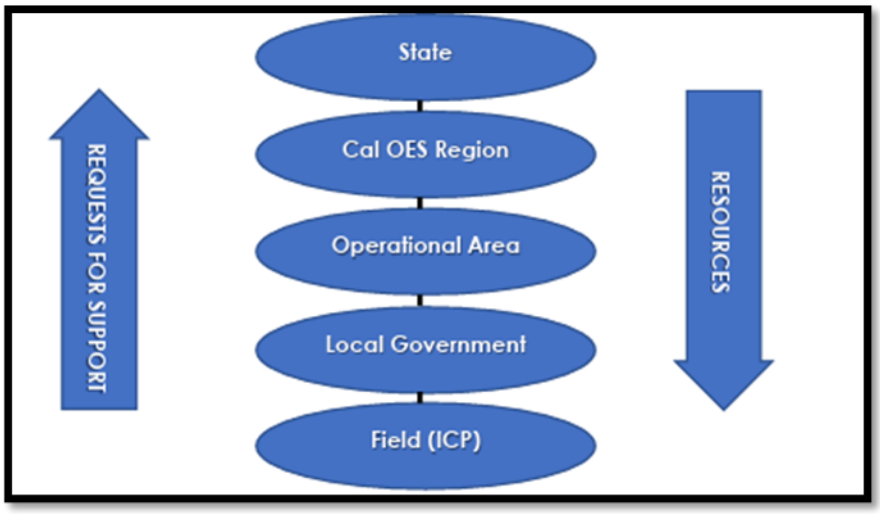


Source: California State Emergency Plan, 2024

5.7.6 EMERGENCY MANAGEMENT COORDINATION

The City's emergency management system operates within the broader SEMS framework, which facilitates coordination of information and resources at the local and regional levels. Graphic 5.7.6 below illustrates this coordinated framework.

Graphic 5.7.6: Emergency Management Coordination



Source: California State Emergency Plan, 2024

5.7.7 STATEWIDE EMERGENCY MANAGEMENT COORDINATION

Cal OES operates three administrative regions—Inland (Sacramento), Coastal (Fairfield), and Southern (Los Alamitos)—which coordinate information and resources across SEMS levels to support local response. These regions represent local perspectives and provide a Cal OES presence throughout all phases of emergency management. The City is part of the Cal OES Southern Region. Graphic 5.7.7 below illustrates the Cal OES Regions.

Graphic 5.7.7: Cal OES Regions

Source: Cal OES

6. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

The City EOC serves as the central hub for collecting, verifying, analyzing, and disseminating emergency information with internal departments, the OA, adjacent jurisdictions, and supporting agencies during City-related incidents. The City is not responsible for managing situational data for emergencies occurring outside its jurisdiction.

Prior to EOC activation, the City may receive alerts and warnings from multiple sources, including the San Bernardino County OES, the San Bernardino County Sheriff's Department Dispatch Center, CONFIRE, the California State Warning Center (CSWC), City departments, neighboring municipalities, utility providers, and the National Weather Service (NWS).

Once activated, the EOC Planning & Intelligence Section leads the collection, evaluation, display, and distribution of incident information, including situational status and resource status. This section supports decision making across the EOC by providing accurate intelligence, anticipating operational developments, producing situation forecasts, and maintaining a common operating picture for all EOC sections.

6.1 OBJECTIVES

Objectives of the information collection, analysis, and dissemination function include, though are not limited to, the following:

- Inform the decision to proclaim local emergencies
- Collect and analyze initial situation reports, including safety conditions and damage assessments
- Display incident data using maps, status boards, and other visual tools within the EOC
- Develop and maintain charts and logs tracking incident status and available resources (personnel, equipment, vehicles, and teams)
- Disseminate intelligence updates to the EOC Director, Management Staff, and General Staff

- Coordinate Geographic Information Systems (GIS) support for mapping and incident documentation
- Prepare and distribute summary reports on safety conditions and damage assessments to EOC Sections, the San Bernardino County EOC, Cal OES, and FEMA
- Document damage levels and develop preliminary financial loss estimates
- Provide situational awareness and planning support to EOC Sections and DOCs
- Develop the City's EOC Action Plan, incorporating input from all sections.
- Coordinate and prepare the City's After-Action Report and Corrective Action Plan following EOC demobilization
- Initiate post-disaster recovery planning and support the transition to a formal Recovery Organization
- Maintain accurate and complete documentation of all EOC activities; ensure record preservation and submit required reports to the San Bernardino County OES, Cal OES, and FEMA
- Identify and coordinate technical experts for specialized topics requiring subject matter expertise
- Provide technical and informational support to the EOC Director for presentations to the City Council, Policy Group, public meetings, and media briefings
- Support mutual aid resource requests and deployments

6.2 INFORMATION COLLECTION

6.2.1 OVERVIEW

Emergency incident information may originate from the following sources:

- Operations Section Branches, including reports from field personnel, DOCs, dispatch centers, and external partners
- Media (television, radio, and print)
- Social media platforms

- Field Observers assigned by the EOC
- Damage Assessment and Damage Inspection Teams
- Situation reports from County, State, and Federal agencies
- Agency representatives assigned to the EOC
- Redlands Emergency Communications Group
- Community-based and neighborhood groups (e.g., CERT, Neighborhood Watch, Neighborhood Associations)
- Preparedness partners such as schools, hospitals, and non-governmental organizations (NGOs)

6.2.2 PRE-EOC ACTIVATION

Prior to EOC activation, incident or situational information may be received from a variety of sources, including:

- San Bernardino County OES
- San Bernardino County EOC
- San Bernardino County Sheriff's Department
- San Bernardino County Fire Protection District
- Consolidated Fire Agencies (CONFIRE)
- Los Angeles Joint Regional Intelligence Center (JRIC)
- California State Warning Center (CSWC)
- City departments and field personnel
- Neighboring jurisdictions
- Utility providers and critical infrastructure partners
- National Weather Service (NWS)

Information is evaluated for accuracy and relevance, then shared with appropriate City officials or departments for situational awareness and potential response coordination.

6.2.3 EOC ACTIVATION

During an EOC activation, the Planning & Intelligence Section is responsible for collecting, analyzing, and displaying accurate and timely information related to the current situation and resource status. This EOC Section ensures that safety and damage assessment data is gathered, compiled, and reported promptly to all EOC Sections, the San Bernardino County OA, and the Cal OES Regions.

The Planning & Intelligence Section coordinates the development of the EOC Action Plan, incorporating input from the EOC Management Section and Section Chiefs to establish operational priorities and guide response activities.

Additionally, the Planning & Intelligence Section manages the Documentation Unit, which is tasked with maintaining detailed records of the emergency response and ensuring those records are preserved for after-action reporting, cost recovery, and historical reference.

The City EOC uses Microsoft platforms (e.g., SharePoint and Teams) for internal incident and resource tracking; WebEOC is used for coordination with the San Bernardino County EOC.

6.3 ANALYSIS AND DISSEMINATION

Analysis: The analysis function transforms raw incident data into actionable intelligence by identifying patterns, assessing impacts, and supporting decision-making across the EOC.

Dissemination: The dissemination function ensures timely, accurate, and targeted delivery of critical information to decision makers, responders, and stakeholders during an emergency.

Once verified, validated, and organized, emergency incident information is disseminated by the EOC Planning & Intelligence Section through multiple channels and formats, including:

- **Internal:** EOC briefings, EOC Action Plans, situation reports, situation displays, internal communications, and EOC Section updates.
- **External:** WebEOC/CalEOC updates, San Bernardino County OA Situation Reports and reporting forms, shared EOC Action Plans, and County emergency management staff assigned to the City EOC.

- **Public:** The PIO coordinates public messaging through the Joint Information System (JIS) or Joint Information Center (JIC) to ensure verified information reaches the public.

THIS PAGE IS INTENTIONALLY LEFT BLANK

7. COMMUNICATIONS

7.1 PUBLIC ALERT AND WARNING

Alert and warning refer to the systems and processes used by government agencies to notify partner organizations and the public of imminent threats or extraordinary hazards. Dependent upon the nature of the threat and the population at risk, alert and warning can originate at any level of government. Protection of life and property is dependent upon timely dissemination of warning and emergency information to the populations in threatened areas.

The City is responsible for alerting and warning within City limits. There are various means and methods whereby an alert or warning may originate and be disseminated to the City and/or San Bernardino County.

7.1.1 RAVE ALERT

The City uses Rave Alert as its emergency mass notification system. The system enables City officials to distribute time-sensitive alerts and public safety information during incidents such as wildfires, floods, hazardous materials incidents, evacuations, and other emergencies.

Notifications, which may be sent as phone calls, text messages, or emails, typically include protective action guidance and other critical information intended to help City residents respond to developing situations.

The Redlands Police Department Communications Unit and Redlands Fire Department/Emergency Management have the ability to send out Rave Alert notifications within City limits.

City residents and employees can register for Rave Alert at https://www.smart911.com/smart911/ref/login.action?pa=cityofredlands.

7.1.2 TELEPHONE EMERGENCY NOTIFICATION SYSTEM

San Bernardino County uses the Telephone Emergency Notification System (TENS), also known as the Reverse 9-1-1 Public Warning System, to deliver rapid emergency notifications to the public. The system alerts County residents to life-threatening incidents such as wildfires, floods, hazardous materials incidents, and other emergencies. The system may provide time-sensitive protective action instructions

including evacuation orders, shelter-in-place directives, or other emergency guidance.

The system enables public safety officials to issue targeted notifications to specific geographic areas based on geocoded addresses and the County's street network. This capability allows alerts to be distributed during both localized and large-scale emergencies.

TENS delivers high-speed notifications through voice and text messaging and is compatible with TDD/TTY devices to support accessible communications.

City residents and employees can register for TENS at https://www.smart911.com/smart911/login.action?lpse=1.

7.1.3 INTEGRATED PUBLIC ALERT AND WARNING SYSTEM

IPAWS is a national FEMA-managed system that allows authorized agencies to issue emergency alerts through multiple channels, including the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), and NOAA Weather Radio. In San Bernardino County, the components of IPAWS are accessed through the TENS portal and require special codes, available through the San Bernardino County Sheriff's Department and San Bernardino County OES, in order to launch messages using its component technologies.

The City may request IPAWS activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.4 EMERGENCY ALERT SYSTEM

7.1.4.1 OVERVIEW

The Emergency Alert System (EAS) enables Federal, State, and local governments to communicate with the public via commercial broadcast stations. Operated voluntarily by broadcasters under Federal Communications Commission (FCC) regulations, EAS disseminates critical emergency information. Message priorities under Part 73.922(a) of the FCC's rules are as follows:

- Priority One: Presidential Messages (live)
- Priority Two: EAS OA (Local) Programming
- Priority Three: State Programming

- Priority Four: National Programming and News

California has 30 EAS OAs within radio reception range of EAS stations serving the area. The State message priorities are as follows:

- Priority One: Immediate action required to save lives
- Priority Two: Property protection and urgent public instructions
- Priority Three: General public information

7.1.4.2 SAN BERNARDINO COUNTY

EAS messages are broadcast in San Bernardino County to all local broadcasters, special districts, and businesses with over 100 employees. Local EAS stations authenticate requests before broadcasting. Authentication details are not released to the public. Emergencies warranting alerts include natural disasters, public safety threats, and hazardous materials incidents.

EAS activation in San Bernardino County can be authorized by the San Bernardino County Sheriff's Department and San Bernardino County OES.

The local EAS stations for southwestern San Bernardino County are:

- Primary Station (LP1): KFRG-95.1 FM
- Alternate Station (LP2): KGGI-99.1 FM

The City may request EAS activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.5 WIRELESS EMERGENCY ALERTS

Wireless Emergency Alerts (WEA) deliver text messages to compatible cellular phones in affected areas, warning users of hazards and providing brief instructions. WEA is enabled by default and does not require opt-in.

WEA messages have the following character limits:

- 360 characters (4G LTE and newer networks)
- 90 characters (3G and older networks)

When sent via IPAWS, alerts are transmitted to cell carriers, which broadcast them from towers in the alert zone. Exact reach is unpredictable due to factors like:

- Geography affecting reception

- Buildings limiting signal penetration
- Device status (powered off or out of battery)
- Towers lacking backup power during outages
- Antenna type (directional vs. omnidirectional) and signal strength

The City may request WEA activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.6 CALIFORNIA STATE WARNING CENTER

The California State Warning Center (CSWC) is the official State level point of contact for emergency notifications. The CSWC maintains contact with OA Warning Points, state agencies, federal agencies and the National Warning Center.

- **Notifications received by CSWC:** Local governments and OAs notify the CSWC of emergencies that affect their community in accordance with existing laws, protocols or when State assistance is requested or anticipated.
- **Earthquake Notifications:** The CSWC receives notifications of earthquakes from the California Integrated Seismic Network (CISN), National Earthquake Information Center (NEIC), and the United States Geological Survey (USGS).
- **Weather Notifications:** Notification of severe weather is received from the NWS San Diego Office.
- **Energy Notifications:** The California Independent Systems Operator (California ISO) monitors the State's power grids.
- **Hazardous Materials, Oil Spill Release Notifications:** In accordance with State law, CSWC will be notified of any release or threatened release of hazardous materials.

The CSWC is responsible for informing, communicating, alerting, and notifying local government, OAs, State officials, and the Federal government of emergencies. The CSWC is equipped with telephone, data, and radio systems, including CALWAS, CLETS, NWS Weather Radio (NWR), Emergency Digital Information Service (EDIS), and Dialogic Emergency Notification System (DENS). Most of these systems are used on a day-to-day basis; others are available for use in an emergency, as conditions require.

- **CALWAS:** The CSWC maintains the California Warning System (CALWAS) to communicate with Cal OES Regional Offices and County Warning Points during an emergency. CALWAS is part of the National Warning System (NAWAS).
- **CLETS:** The California Law Enforcement Telecommunications System (CLETS) is a high-speed message switching system that provides law enforcement and criminal justice agencies with the capability of obtaining information directly from Federal, State, and local computerized information files. In addition, the system will provide fast and efficient point-to-point delivery of messages between agencies.
- **OASIS:** Cal OES leases transponder space from a commercial satellite operator and operates a satellite communications system known as Operational Area Satellite Information System (OASIS). This system serves as one of the back-up and redundancy systems and allows public safety agencies to exchange disaster intelligence and resource requests when the Public Switched Telephone Network (PSTN) fails. In the event of PSTN failure, OASIS is the primary back-up, providing voice and internet connectivity with the CSWC, Cal OES REOCs, key State agencies, and each OA.

7.1.7 NATIONAL WEATHER SERVICE

National Weather Service (NWS) provides weather forecasts and warnings to the nation. The City and southwestern San Bernardino County receive notifications from the San Diego Forecast Office.

NWS transmits continuous weather information for the San Bernardino County area on 162.450 MHz. The NWS severe weather broadcasts are preceded with a 1050 MHz tone that activates weather monitor receivers equipped with decoders. The NWS can also access NAWAS to announce severe weather information, which is disseminated to the county warning points using the CALWAS system.

The levels of notifications that the NWS issues include the following:

- **Outlook:** Indicates the potential for hazardous weather over the coming days, intended to provide advance awareness with low certainty and no immediate action required.
- **Statement:** Provides additional information, updates, or clarification about ongoing or recent weather conditions.

- **Watch:** Indicates that conditions are favorable for a specific hazard to develop, meaning individuals should remain alert and prepared to take action.
- **Advisory:** Indicates that weather conditions that may cause inconvenience or minor impacts, requiring caution but typically not posing a significant threat to life or property.
- **Warning:** Indicates that a hazardous event is imminent or occurring, requiring immediate protective action.

7.1.8 ROUTE ALERTING AND DOOR-TO-DOOR CANVASSING

The City may use route alerting and door-to-door canvassing to alert and notify the public. Route alerting is commonly used in small-scale emergencies or rapidly evolving situations within a defined area. It involves emergency officials driving or walking through the affected zone to inform residents of the situation and recommended actions. This can be done door-to-door or via public address systems on police or fire vehicles.

While effective, especially when other systems are unavailable, route alerting depends on resource availability and can be time-consuming. It is typically used in localized settings such as neighborhoods, apartment complexes, mobile home parks, hotels, and college campuses. Route alerting can also serve as a supplement to other alert and warning methods.

7.2 COMMUNICATION SYSTEMS

7.2.1 TELEPHONES

The City EOC has one dedicated VoIP phone, with additional VoIP phones available in the room through the Redlands Police Department. Conference call phones and numbers can be provided as needed. Requests for any additional telecommunications support should be routed to the EOC Logistics Section, Communications Unit.

7.2.2 CELLULAR PHONES

The City maintains cellular service through multiple providers, and City-issued cell phones are assigned to staff for use in the EOC and during emergency operations. These phones support voice, text, and data and serve as a backup to landline and

radio systems. During major incidents, network congestion may occur, so staff should use text messaging when possible to improve reliability.

7.2.3 EMAIL

Email is a redundant method of communication between the OA EOC and the City EOC due to the number of reporting jurisdictions and the quantity of documentation provided. Like cellular telephones, if other primary means of data or voice communications fail, then email should be considered a sufficient back-up. Before using email, however, personnel should confirm that the intended recipient(s) has access to and is checking their email. Critical information should never be sent over email unless confirmation exists that the intended recipient is receiving the messages.

7.2.4 800 MHZ RADIOS

The City EOC has connectivity to San Bernardino County's 800 MHz system, which provides access from the EOC to field personnel (e.g., fire, police, public works, public utilities, etc.) and potentially to mutual aid partners. During an emergency, City radios should be limited to emergency radio traffic only.

7.2.5 SATELLITE TELEPHONES

The City has four portable satellite phones for communicating with other cities and agencies belonging to the emergency managers talk group. Satellite phones use a geostationary satellite above Earth as a repeater and serve as backup communication if other systems fail.

Two units are assigned to the Redlands Fire Department (Fire Chief and Emergency Management), and two units are assigned to the Redlands Police Department (Communications Unit and Mobile Command Post).

7.2.6 REDLANDS EMERGENCY COMMUNICATIONS GROUP

The Redlands Emergency Communications Group (RECG), also known as the Radio Amateur Civil Emergency Service (RACES), consists of volunteer amateur radio operators who are committed to assisting with emergency communications in times of disaster. RECG is managed by the Fire Department and provides auxiliary communications support for EOC operations, field operations, and City departments.

7.2.6.1 SAN BERNARDINO COUNTY RACES

San Bernardino County maintains a cadre of RACES volunteers and radio base stations to ensure communications between the OA EOC and various locations can be maintained. Individual operators may have their own base stations that can also be dispatched at the discretion of the OA EOC. Emergency information can be communicated through RACES operators to any location where an operator is dispatched (e.g., mutual aid EOCs, Incident Command Posts, shelters, staging areas, etc.). Emergency information of any sort may be communicated through a ham radio operator.

While operating in a RACES capacity, stations and amateurs registered with the local RACES organization may not communicate with amateurs who are not operating in that capacity.

7.2.7 INLAND SOCAL 211

The 211 system is an FCC-designated, three-digit number that connects the public to community, health, and social service resources; it is not a dispatch line like 911, 988, or 311, though it can support emergencies by providing verified information and referrals. Inland SoCal 211, operated by the Inland Southern California United Way, offers 24/7 access to services and helps San Bernardino County residents during emergencies in coordination with the American Red Cross (ARC) and other partners.

7.2.8 RELAY SERVICES

California Connect provides a statewide telecommunications relay service that enables California residents with speech, hearing, vision, mobility, or cognitive disabilities to connect using functional equivalent equipment and services. The service offers voice-to-text, text-to-voice, and other assistive communication options to ensure accessible and reliable communication during emergencies and routine operations. This service is available by dialing 7-1-1.

7.2.9 WEBEOC

San Bernardino County OES uses WebEOC as its crisis information management system. WebEOC is a web-based platform that enables secure, real-time information sharing and resource coordination during disasters and emergencies.

The City uses WebEOC to:

- Share situational status information with San Bernardino County
- Coordinate resource requests with San Bernardino County

7.3 PUBLIC INFORMATION

7.3.1 CITY BROADCAST

The City operates a broadcast channel called Redlands TV, which features live and recorded meetings, community programming, and special events coverage.

Redlands TV is available to cable television subscribers through Spectrum cable (Channel 3) or Frontier cable (Channel 35) services and is also hosted online at https://www.redlands.gov/redlands-tv.

7.3.2 SOCIAL MEDIA

The City utilizes its website and social media platforms to reach the public. In an emergency or disaster, the City EOC will post information on these accounts and monitor these accounts for messages and information from the public.

- City Website: https://www.redlands.gov
- Facebook: https://www.facebook.com/cityofredlands
- Instagram: https://www.instagram.com/cityredlands
- X (formerly Twitter): https://x.com/cityofredlands

7.3.3 MEDIA BRIEFINGS AND PUBLIC MEETINGS

The City may hold media briefings and community meetings before, during, and after emergencies to provide essential updates. Accessibility measures will include sign language interpreters, large-print materials, and translation services.

During EOC activations, the Public Information Officer (PIO) will develop key messages, anticipate public questions, and highlight response and recovery efforts.

THIS PAGE IS INTENTIONALLY LEFT BLANK

8. MUTUAL AID AND RESOURCE MANAGEMENT

8.1 MUTUAL AID OVERVIEW

California's basis for mutual aid is the California Civil and Defense Master Mutual Aid Agreement (MMAA), through which the State, its agencies, political subdivisions, public agencies, and federally recognized tribes agree to support one another when local resources are insufficient. The MMAA requires signatories to provide assistance without expectation of reimbursement, although federal or State funding may reimburse eligible costs. Assistance provided under other agreements, memoranda, or contracts is governed by the terms of those documents.

Mutual aid requests follow established, discipline-specific procedures and are routed through designated mutual aid coordinators, who manage resource requests within their areas and elevate them to the next level of government when necessary.

The City of Redlands participates in California's mutual aid system to ensure rapid access to additional personnel and resources during major incidents and to provide reciprocal support to neighboring jurisdictions when their needs exceed local capacity. Through this system, Redlands benefits from statewide surge capability and, when it deploys resources to assist others, the City is eligible to recover its allowable response costs plus any approved administrative overhead in accordance with California mutual aid reimbursement policies.

8.2 MUTUAL AID AGREEMENTS

Mutual aid agreements are fundamental to effective emergency management, enhancing resource availability and improving the City's capacity to respond to and recover from disasters.

Mutual aid assistance within California is provided under the following authorities:

- California Civil and Defense Master Mutual Aid Agreement
- California Fire and Rescue Mutual Aid Plan
- California Urban Search and Rescue Mutual Aid Plan
- California State Mutual Aid Pre-Position Program

- California Law Enforcement Mutual Aid Plan
- California Search and Rescue Mutual Aid Plan
- California Coroner Mutual Aid Plan
- California Public Health and Medical Assistance
- California Emergency Managers Mutual Aid (EMMA)
- California Public Works Mutual Aid Agreement

Mutual aid assistance between states may be provided under the following authorities:

- Emergency Management Assistance Compact (EMAC)
- Robert T. Stafford Disaster Relief and Emergency Assistance Act

8.3 CALIFORNIA MUTUAL AID FRAMEWORK

8.3.1 STATE MUTUAL AID PROVISIONS

State agencies may provide mutual aid—personnel, equipment, and other resources—to support political subdivisions during a Local Emergency, under existing mutual aid agreements, or at the Governor's direction. This authority enables the City to receive direct State assistance when local and County resources are exceeded.

8.3.2 MUTUAL AID CHARGES AGAINST THE STATE

In the absence of a State of War Emergency or State of Emergency, the cost of extraordinary services incurred by political subdivisions in executing mutual aid agreements constitutes a legal charge against the State when approved by the Governor under orders and regulations issued pursuant to California Government Code § 8567. This provision allows the City to receive State reimbursement for eligible extraordinary mutual aid costs incurred outside a declared state emergency.

8.3.3 CALIFORNIA MUTUAL AID PROGRAMS

The State's mutual aid programs, which are coordinated by Cal OES and the Emergency Medical Services Authority (EMSA), are summarized in Table 8.3.3 on the next page.

Table 8.3.3 California Mutual Aid Programs

CALIFORNIA MUTUAL AID PROGRAMS MUTUAL AID SYSTEMS AND CHANNELS OF STATEWIDE MUTUAL AID COORDINATION			
COORDINATED BY CAL OES			COORDINATED BY EMSA
Fire & Rescue	**Law Enforcement**	**Emergency Management**	**Disaster Medical & Health**
Fire & Rescue Mutual Aid	Coroner Mutual Aid	Public Works Mutual Aid	Medical Mutual Aid
Urban Search & Rescue Mutual Aid	Law Enforcement Mutual Aid	California Water/Wastewater Agency Response Network (CalWARN)	
	Search & Rescue Mutual Aid (non-urban)	Emergency Managers Mutual Aid (EMMA)	

8.3.4 CALIFORNIA MUTUAL AID REGIONS

The State of California is divided into three Administrative Regions and six Mutual Aid Regions to coordinate mutual aid. The City is in Mutual Aid Region VI within the Southern Administrative Region.

A Mutual Aid Region is a subdivision of Cal OES established to facilitate coordination of mutual aid and emergency operations within an area of the State consisting of two or more county OAs. An OA is an intermediate level of the state emergency services organization consisting of a county and all political subdivisions within that county.

Cal OES Mutual Aid and Administrative Regions are illustrated in Graphic 8.3.4 on the next page.

Graphic 8.3.4 Cal OES Mutual Aid and Administrative Regions

Source: Cal OES

8.3.5 MUTUAL AID COORDINATION

Mutual aid systems work through designated Mutual Aid Coordinators at the local agency, OA, regional, and State levels. Mutual Aid Coordinators receive requests, coordinate the provision of resources within their designated geographic areas of responsibility, and send unfilled requests to the next level of coordination.

8.3.6 LOCAL CONTROL

The City will retain command of incidents within its jurisdiction that require mutual aid, consistent with California Government Code § 8618:

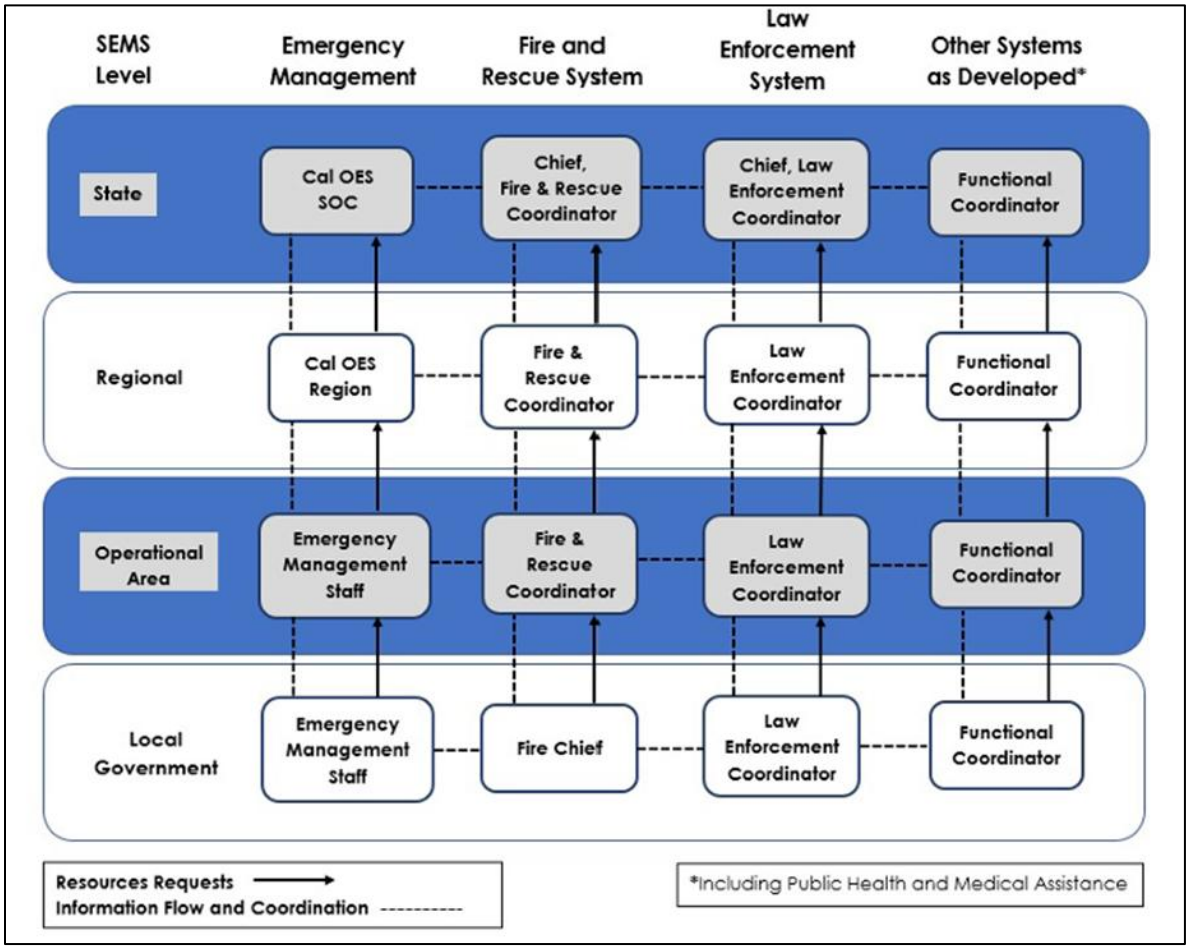
"Unless otherwise expressly provided by the parties, the responsible local official in whose jurisdiction an incident requiring mutual aid has occurred shall remain in charge at such incident, including the direction of personnel and equipment provided to him through mutual aid."

8.3.7 DISCIPLINE-SPECIFIC MUTUAL AID COORDINATION

The statewide mutual aid system incorporates several discipline-specific mutual aid systems, including Fire and Rescue, Law Enforcement, and Emergency Management. Fire and Rescue Mutual Aid Coordinators and Law Enforcement Mutual Aid Coordinators are designated at the OA, regional, and State levels to support mutual aid coordination during both routine and large-scale public safety incidents. Regional Disaster Medical Health Coordinators are also assigned within each mutual aid region to coordinate medical mutual aid. Mutual aid requests outside these discipline-specific systems are coordinated through EMMA by emergency management personnel at the local, OA, regional, and State levels.

Discipline-specific mutual aid systems are illustrated in Graphic 8.3.7 below.

Graphic 8.3.7 Discipline-Specific Mutual Aid Coordination



Source: Cal OES

8.4 CITY MUTUAL AID PARTICIPATION

The City participates in multiple statewide, regional, and industry mutual aid systems. Participation in these **State systems** is coordinated by the City departments listed in Table 8.4.

Table 8.4 California Mutual Aid Program Participation

CA MUTUAL AID PROGRAM	RESPONSIBLE CITY DEPARTMENT
Fire & Rescue	Fire Department ▪ On-Duty Battalion Chief
Law Enforcement	Police Department ▪ Watch Commander
Public Works	Facilities & Community Services Department ▪ Director
Utilities (Water & Electric)	Municipal Utilities & Engineering Department ▪ Director
Emergency Managers Mutual Aid (EMMA)	City Manager's Office / Fire Department ▪ City Manager, Assistant City Manager, Fire Chief, or their designee

8.4.1 CITY MUTUAL AID COORDINATION

Participation in all mutual aid programs, including **statewide, regional, and industry mutual aid systems**, is coordinated by the City departments listed in Table 8.4.1.

Table 8.4.1 City Mutual Aid Coordination

MUTUAL AID PROGRAM	RESPONSIBLE CITY DEPARTMENT
American Water Works Mutual Aid (via CalWARN)	Municipal Utilities & Engineering Department
California Master Mutual Aid Agreement (MMAA)	City Manager's Office / Fire Department
California Utilities Emergency Association (CUEA) **Mutual Aid**	Municipal Utilities & Engineering Department
California Water/Wastewater Agency Response Network (CalWARN)	Municipal Utilities & Engineering Department
Coroner Mutual Aid	Police Department (via San Bernardino County Sheriff's Department)
Edison Electric Institute Mutual Aid	Municipal Utilities & Engineering Department (as coordinated through SCE)
Emergency Managers Mutual Aid (EMMA)	City Manager's Office / Fire Department
Emergency Response Network of the Inland Empire (ERNIE) **Mutual Aid**	Municipal Utilities & Engineering Department, and Fire Department Emergency Management Division
Law Enforcement Mutual Aid (LEMA)	Police Department
Medical Mutual Aid	Fire Department (via CONFIRE Communications Center)

Public Health Mutual Aid	Fire Department (via SBCO DPH)
Public Power Mutual Aid	Municipal Utilities & Engineering Department (as coordinated through SCE)
Public Works Mutual Aid	Facilities & Community Services Department
Search and Rescue Mutual Aid	Police Department
Urban Search and Rescue Mutual Aid	Fire Department
Western Region Mutual Assistance Group (WRMAG)	Municipal Utilities & Engineering Department (as coordinated through SCE)

8.4.2 EMERGENCY RESPONSE NETWORK OF THE INLAND EMPIRE

The City is a member of the Emergency Response Network of the Inland Empire (ERNIE), which was established in 2006 and operates within Riverside and San Bernardino Counties. ERNIE is a consortium of public agencies that facilitates preparedness, response, and recovery for local and regional disasters and supports continuity of critical public services. Through a formal mutual assistance agreement, ERNIE member agencies provide personnel, equipment, and other resources to jurisdictions when incidents exceed local capabilities, consistent with applicable State and Federal requirements, and support training, interoperable communications, reimbursement documentation, and After-Action Report/ Improvement Plan (AAR/IP) development.

8.5 EMERGENCY MANAGEMENT ASSISTANCE COMPACT

The Emergency Management Assistance Compact (EMAC) is a congressionally ratified interstate mutual aid agreement that provides the structure and procedures for states and territories to request and render emergency assistance. California is a member of EMAC. Once the Governor proclaims a State of Emergency, California may request and receive assistance from other EMAC member states. The Director of Cal OES, supported by the State's EMAC Coordinator, is responsible for facilitating EMAC requests and deployments.

The City may request or receive assistance through the Emergency Management Assistance Compact (EMAC) when coordinated by Cal OES, which serves as the State's EMAC authority.

8.6 RESOURCE MANAGEMENT OVERVIEW

The City will manage local and mutual aid resources in accordance with SEMS and NIMS.

Resource management during incidents will include:

- **Identification and Typing of Resources** – City departments will maintain current inventories of personnel, equipment, facilities, and supplies. Where applicable, inventories will be kept consistent with Cal OES and FEMA resource typing standards.
- **Request and Coordination** – City requests for **non-mutual-aid resources** go through the City EOC and are coordinated by the EOC Logistics Section. **Mutual aid requests** move through the appropriate discipline-specific mutual aid system and are coordinated by Mutual Aid Coordinators at the City, County, regional, and State levels.
- **Resource Tracking** – **Non-mutual-aid resources** are tracked by the EOC using established EOC resource management tools for status, location, and assignment. **Mutual aid resources** are tracked within the respective discipline-specific mutual aid system using that system's established tracking processes.
- **Demobilization and Return** – **Non-mutual-aid resources** are demobilized through the EOC and released as soon as they are no longer required, then returned in the condition received unless otherwise specified. **Mutual aid resources** are demobilized through their respective mutual aid systems and released according to that system's established procedures, with resources returned in the condition received unless otherwise specified.
- **Documentation** – Resource requests and utilization will be documented by the requesting department and the City EOC to ensure accountability and to support reimbursement through programs such as the California Disaster Assistance Act, the California Fire Assistance Agreement, and applicable federal reimbursement programs.

8.6.1 RESOURCE PRIORITIZATION

When resource availability is limited, priority will be given to:

1. Protection of life
2. Protection of property and the environment
3. Incident stabilization

When the City EOC is not activated, City resource allocation decisions will be managed by the appropriate City department, while mutual aid resource allocation decisions will be coordinated through the appropriate Mutual Aid Coordinator.

When the City EOC is activated, City resource allocation decisions will be coordinated by the EOC Director in consultation with the Operations Section and Logistics Section Chiefs, while mutual aid resource requests and allocations will continue to be processed through the applicable mutual aid system and its designated Mutual Aid Coordinators.

8.6.2 RESOURCE ORDERING AND TRACKING

The City will order, assign, and track City resources using local systems and processes. Mutual aid resources will be requested, coordinated, and tracked through the applicable discipline-specific mutual aid systems and their designated Mutual Aid Coordinators.

When City resources are insufficient or additional support is required, the City EOC will submit and track resource requests through the County's WebEOC platform, which provides centralized, real-time coordination of personnel, equipment, and supplies.

The City remains accountable for resources not tracked by other entities and will monitor the following for each resource:

- Current status (available, assigned, out of service)
- Location and mission assignment
- Estimated time of arrival and assignment duration

Resource tracking may also be supported through:

- Digital EOC (City EOC Microsoft Teams account)
- Incident/EOC Check-In Lists

- Resource Request Message Forms
- Resource Status Cards (T-Cards)
- Other approved EOC tracking tools or technology

8.6.3 INTEGRATION WITH PRIVATE SECTOR AND NON-GOVERNMENTAL ORGANIZATIONS

The City may also access resources from the private sector, non-governmental organizations, and community partners to supplement operations. Examples include:

- Pre-approved or contracted vendors for emergency supplies, fuel, transportation, etc.
- The American Red Cross and other partners for sheltering and feeding
- Faith-based organizations, businesses, and volunteer groups within the City that support emergency response and recovery

8.6.4 RESOURCE DEMOBILIZATION

- **City (non-mutual-aid) resources** are released promptly when no longer required and demobilized through the City's internal processes, coordinated by the Logistics Section in consultation with the Operations Section.
- **Mutual aid resources** are released when no longer required and demobilized through the same mutual aid channels used for their request, in coordination with the appropriate Mutual Aid Coordinator.
- **All released resources** are documented, and any repair or replacement agreements are managed by the EOC Finance & Administration Section. Resources are returned to their point of origin in the condition received unless otherwise stated.

THIS PAGE IS INTENTIONALLY LEFT BLANK

9. CONTINUITY OF GOVERNMENT

The Continuity of Government concept comprises three elements:

1. Standby Officers for the Governing Body
2. Temporary Seat of Government
3. Preservation of Vital Records

An emergency or disaster could result in the injury or death of key government officials, the partial or complete destruction of established seats of government, and the destruction of public and private records essential to government operations.

Government at all levels is responsible for providing continuity of effective leadership and authority, direction of emergency operations, and management of recovery operations. To this end, the City must continue functioning as a governmental entity during and after an emergency or disaster. The California Government Code and the Constitution of California provide the authority for State and local government to reconstitute if key officials are unavailable or unable to serve.

Continuity of operations (COOP), not the subject of this EOP, consists of additional operational, logistical, and procedural elements.

9.1 RECONSTITUTION OF GOVERNMENT

California Government Code, Title 2, Division 1, Chapter 7, Article 15 ("Preservation of Local Government") establishes the primary statutory framework for continuity and reconstitution of local government in California during attack, state of emergency, or local emergency.

Article 15 contains the following provisions:

- **§8635 – Purpose:** Ensures continuity of local government during enemy attack or emergencies to preserve law and order and restore services.
- **§8636 – Definition of "Unavailable":** An officer is unavailable if killed, missing, or seriously injured; governing body decides.
- **§8637 – Succession Authority:** Political subdivisions may establish succession for department heads critical to law and safety.

- **§8638 – Standby Officers:** Governing bodies have the authority to appoint three standby officers for each member and for the chief executive.
- **§8639 – Qualifications:** Standby officers' suitability must be investigated, considering residence and work for survivability.
- **§8640 – Oath & Tenure:** Standby officers take the same oath as regular officers; serve at the pleasure of the governing body.
- **§8641 – Duties:** Standby officers must learn the role, stay informed, report for duty in emergencies, and fill posts in succession until regular officers return or replacements are chosen.
- **§8642 – Governing Body Meetings:** Must convene promptly during emergencies, even outside jurisdiction; if only one member remains, that member may reconstitute the body.
- **§8643 – Governing Responsibilities:** Assess damage, reconstitute itself and the political subdivision, and resume law and order and services.
- **§8644 – Temporary Officers:** If all governing and standby members are unavailable, temporary officers are appointed by county supervisors or nearby mayors, in order of proximity and population.

The City's municipal code (MC Chapter 2.52) establishes the primary legal framework for the City's continuity of government. The City maintains separate citywide and departmental policies and procedures that support continuity of government and continuity of operations.

9.2 DIRECTOR OF EMERGENCY SERVICES

MC § 2.52.080 designates the City Manager as the Director of Emergency Services.

Should the Director of Emergency Services be unable to serve, the Assistant City Manager(s) will automatically succeed until a permanent successor has been appointed by the City Council and seated. The Assistant City Manager(s) will have all the authority and powers of the Director of Emergency Services.

9.3 SUCCESSION OF OFFICERS

9.3.1 SUCCESSION OF CITY COUNCIL

The emergency interim succession of the City Council is permitted by California Government Code § 8638, which states:

"To provide for the continuance of the legislative and executive departments of the political subdivision during a state of war emergency or a state of emergency or a local emergency the governing body thereof shall have the power to appoint the following standby officers: (a) Three for each member of the governing body. (b) Three for the chief executive, if he is not a member of the governing body."

The City's succession list, consistent with California Government Code § 8638, is on file with the City Clerk.

9.3.2 SUCCESSION OF KEY CITY OFFICIALS

The following staff positions are key to emergency operations. The City has identified standby officers if a member is unavailable or unable to serve during a proclaimed emergency or disaster. Emergency interim lines of succession are identified in separate City policies and procedures. The succession list consistent with this section is on file with the City Clerk.

As used in this plan, the word "unavailable" means that a department head or other key City official is missing, seriously injured, deceased, or otherwise indisposed and cannot attend meetings or otherwise perform their duties. The City Manager will settle any question as to whether a particular member is unavailable.

Key positions identified as requiring emergency interim successors include:

- City Manager
- Assistant City Manager(s)
- City Attorney
- City Clerk
- Fire Chief
- Chief of Police
- Municipal Utilities & Engineering Director

- Facilities & Community Services Director
- Chief Information Officer
- Finance Director
- Human Resources Director
- Development Services Director
- Library Director
- Chief Building Official

Individuals designated as temporary successors for the above positions will immediately assume all authorities, powers, and duties of those positions when necessary.

9.4 ALTERNATE SEAT OF GOVERNMENT

The City's seats of government are provided in Table 9.4. The City also maintains virtual and remote work capabilities.

Table 9.4 City Seats of Government

CITY SEATS OF GOVERNMENT	
PRIMARY SEAT	**ALTERNATE SEAT**
City Hall 35 Cajon St, Suite 200 Redlands, CA 92373	**A.K. Smiley Public Library** 125 W Vine St Redlands, CA 92373

9.5 PRESERVATION OF VITAL RECORDS

The City is responsible for establishing measures that ensure the preservation and protection of vital records. Each department within the City will identify, maintain, and protect its vital records. Vital records are defined as those records that are essential to the rights and interests of the City, personnel, individuals, corporations and other entities, including vital statistics, land and tax records, personnel record, articles of incorporation, and historical information. Vital records also include those records essential for emergency response and recovery operations, including utility system maps, emergency supply and equipment locations, emergency operations plans and procedures, and personnel databases.

These vital records will be essential to the re-establishment of normal functions, serving to protect the rights and interests of the City. These rights and interests may include the constitution, charters, statutes, ordinances, resolutions, court records, official proceedings, and financial records of the City. The City Clerk and Deputy City Clerk, as the custodians of vital records, are responsible for maintaining, securing, and protecting all permanent records necessary for the continuity of City government.

THIS PAGE IS INTENTIONALLY LEFT BLANK

10. ADMINISTRATION, FINANCE, AND LOGISTICS

Emergency operations will be supported by the City's administrative, financial, and logistical procedures, resources, and personnel. In many cases, departments will use the same procedures and processes during emergency operations that are used during daily operations to manage similar functions. In other cases, unique emergency-specific procedures and protocols will be applied or developed to meet the needs of the emergency.

10.1 ADMINISTRATIVE PRACTICES

Adhering to established administrative and financial practices is essential for accurate resource tracking, reimbursement, and after-action reporting. City departments maintain internal procedures to support these functions, including tracking expenditures, managing resource requests, recording training, and documenting emergency exercises.

During emergencies, City departments may modify or temporarily suspend routine administrative procedures when necessary to support response and recovery operations. Such adjustments should be deliberate and guided by the City's Proclamation of Emergency, the EOC Action Plan, and the procedures outlined in this plan.

10.2 DOCUMENTATION

Timely and accurate documentation of emergency incidents is essential for conducting after-action reviews, supporting cost recovery, and legal protection. City departments are responsible for maintaining records that support these functions, including tracking expenditures, documenting recovery efforts, and preserving information for potential litigation.

When activated, the EOC Finance & Administration Section is responsible for maintaining records related to damage costs, expenditures, cost recovery, insurance claims, personnel overtime, and other emergency-related expenses. Guidance for these responsibilities is provided in the EOC Finance & Administration Section position checklists in **Part 2 (Position Checklists)** of this plan.

When activated, the Documentation Unit of the EOC Planning & Intelligence Section is responsible for collecting and maintaining all other incident records and documents.

10.2.1 AFTER-ACTION REPORTS

California Code of Regulations, Title 19, § 2450 requires any city or county declaring a local emergency for which the Governor also proclaims a State of Emergency to submit an After-Action Report to Cal OES within 90 days after the close of the incident period.

An After-Action Report serves the following important functions:

- Provides a source for documenting response and early recovery activities
- Identifies problems and successes during emergency operations
- Analyzes the effectiveness of the different SEMS components
- Identifies, documents, and facilitates corrective action for implementing and tracking improvements to existing emergency response and recovery efforts

The Fire Chief as the Emergency Manager (or designee) is responsible for coordinating the After-Action Review process and ensuring the After-Action Report is submitted.

10.3 FINANCE DURING DISASTERS

10.3.1 EMERGENCY FUNDS

Financial support for emergency response and recovery operations will generally be from funds regularly appropriated to City departments. If the demands exceed available funds, the City Manager may make additional funds available from reserve emergency funds. In that case, the City Manager has the authority under a Proclamation of Local Emergency to transfer and expend money appropriated for other purposes. Emergency expenditures will be made under the authority of the City Manager/Director of Emergency Services (MC § 2.52.100, MC § 2.52.130) unless otherwise authorized by City policy or emergency actions. Emergency finance and procurement activities will be conducted in accordance with MC § 2.16.130 and the City of Redlands Purchasing Guidelines and Procedures (February 2026).

10.3.2 DISASTER COST ACCOUNTING

Disaster-related expenditures may be eligible for reimbursement under various State and Federal programs, but the process requires thorough documentation and accurate recordkeeping to maximize recovery for eligible costs. The Finance

Department leads the City's efforts to apply for reimbursement, which can span years when infrastructure damage is extensive. Eligible costs must be directly related to the disaster response and include expenses that are reasonable, necessary, and compliant with procurement requirements. These typically cover direct costs such as salaries, equipment, materials, and contracts but exclude items like standby costs and lost revenue.

To secure funding, departments must maintain detailed records tied to original source documents from the start of the emergency. This includes payroll records, equipment logs, contractor documentation, procurement justifications, and purchase agreements. The Finance Department initiates tracking codes for emergency costs, while the EOC Finance & Administration Section compiles and submits expenditure summaries. All data must align with grant guidelines, such as those in FEMA's Public Assistance Program and Policy Guide, to ensure claims are fully supported and reimbursable.

10.4 LOGISTICS

Logistics encompasses the acquisition, tracking, and use of services, supplies, and equipment to support the EOC Action Plan and achieve emergency response and recovery objectives. The City Fire Department's Emergency Management Division leads the City's logistical preparedness and readiness activities before an emergency. City departments are responsible for planning for and having access to the emergency logistics required to carry out their assigned roles within the EOP.

When the EOC is activated, the EOC Logistics Section coordinates the acquisition, deployment, tracking, and utilization of emergency logistics to support operational priorities.

10.4.1 CITY DEPARTMENT LOGISTICS

During the preparedness phase of emergency management, City departments should take the following steps:

- Maintain current inventories of locally available resources, including equipment, personnel with specialized technical skills, supplies, and facilities
- Develop and maintain lists of out-of-area resources and mutual aid partners, including supporting agreements (e.g., MOUs, MAAs)
- Conduct just-in-time updates to all resource databases and ensure copies are transferred to the EOC in advance of or immediately prior to an emergency

- Review and test resource procurement processes, including emergency purchasing protocols and continuity of supply chains

10.4.2 EOC LOGISTICS

When activated, the EOC Logistics Section will coordinate all logistical support activities. Responsibilities include:

- Procuring, allocating, tracking, and demobilizing resources
- Coordinating personnel, facilities, equipment, supplies, and services
- Managing transportation, communications, food services, and lodging for response personnel
- Ensuring resource availability and identifying shortfalls or capability gaps

10.4.3 LOGISTICS DATABASES

Logistics and resource databases, lists, and rosters will be maintained in Digital EOC by the City Fire Department's Emergency Management Division and other City departments, including, though not limited to:

- Typed resources maintained by City departments, consistent with FEMA/NIMS resource typing standards
- Vendor and suppliers of emergency equipment and supplies
- Credentialed emergency management personnel
- Emergency facilities (e.g., shelters, staging areas, points of distribution)
- Personnel roster for deployment and staffing support
- Inventory of expendable emergency supplies (e.g., fuel, medical supplies, Personal Protective Equipment [PPE])
- Inventory of emergency sustenance supplies for EOC and field staff (e.g., food, water, hygiene items)

11. TRAINING AND EXERCISE

Training is essential for preparing public officials, emergency managers, and response personnel for disaster operations. A performance-based training program should be conducted regularly to ensure that existing staff maintain operational readiness and that new personnel gain the skills and knowledge needed to carry out their emergency responsibilities effectively.

By maintaining and adhering to a comprehensive training and exercise program, City personnel remain prepared to implement the EOP and carry out their assigned emergency responsibilities effectively.

11.1 EMERGENCY OPERATIONS TRAINING

Emergency operations training is essential to ensuring that personnel are adequately prepared to carry out their assigned emergency roles and responsibilities. The City Manager/Director of Emergency Services is ultimately responsible for ensuring the disaster readiness of City staff. City departments are responsible for scheduling and documenting the training of their respective personnel.

Personnel assigned to the City EOC should be trained for the positions they are expected to fill, consistent with the principles of SEMS and NIMS. Minimum recommended training for personnel assigned to the City's EOC are outlined below and accessible online:

- SEMS G606 (SEMS Introduction)
- IS-100 (Introduction to ICS)
- IS-200 (Basic ICS for Initial Response)
- IS-700 (An Introduction to the National Incident Management System)
- IS-800 (National Response Framework, An Introduction)
- IS-2200 (Basic Emergency Operations Center Functions)

Other position-specific training may be required for certain EOC roles, not limited to the Public Information Officer, EOC Manager, Cost Unit Leader, and Command and General Staff positions. A comprehensive and up-to-date EOC training plan is on file with, and maintained by, the Redlands Fire Department's Emergency Management Division.

The City will coordinate additional training, including training in EOC management/operations and EOC position-specific training, to ensure a trained and capable EOC Response Team. Regular refresher training is recommended for all EOC personnel, supplemented by specialized and just-in-time training based on evolving threats and operational requirements.

FEMA maintains training and credentialing frameworks under NIMS, including the National Qualification System (NQS). Cal OES provides SEMS training guidance and course standards that support local agency qualification and preparedness efforts. These may all serve as benchmarks for developing and maintaining EOC personnel qualifications. Further, the City will meet applicable training and exercise requirements tied to Federal preparedness grants.

Additional emergency operations training opportunities and courses are available from the following sources:

- Cal OES California Specialized Training Institute (CSTI)
- National Disaster & Emergency Management University through its online Independent Study Program
- Riverside Urban Area Security Initiative (UASI)

11.2 EMERGENCY OPERATIONS EXERCISES

Emergency operations exercises are essential for validating emergency operations training and providing City staff with an opportunity to carry out their assigned emergency roles and responsibilities in a safe, low-stress environment. Exercises provide a controlled environment for personnel to become proficient in emergency procedures, facilities, and systems. Local municipalities should participate in all-hazards exercises in coordination with emergency management and first response agencies, emphasizing sustained operations conducted over extended durations.

The City conducts emergency operations exercises to validate emergency plans and procedures, define section-and position-specific responsibilities, test equipment and systems, and ensure the readiness of assigned emergency personnel. City-led exercises will be conducted in accordance with SEMS, NIMS, and the Homeland Security Exercise and Evaluation Program (HSEEP), using a progressive planning approach from discussion-based to operations-based formats.

Discussion-based exercises include:

- **Seminars:** Introduce or review plans, policies, and procedures.
- **Workshops:** Build consensus, develop plans, or refine procedures.
- **Tabletop Exercises (TTX):** Explore hypothetical scenarios and test decision-making.
- **Games:** Explore decision-making and consequences in a competitive environment.

Operations-based exercises include:

- **Drills:** Test a single operation or function.
- **Functional Exercises (FE):** Test command, control, and coordination in a simulated environment.
- **Full-Scale Exercises (FSE):** Evaluate full response capabilities with deployment of personnel and equipment.

Exercises must have clearly defined objectives that relate to one or more of FEMA's Core Capabilities from the National Preparedness Goal. These capabilities span all phases of emergency management.

Exercises should include a plan for observing and assessing performance against the stated objectives. This is accomplished by exercise evaluators, who take notes, track timelines, and measure how well participants execute their roles.

After every exercise, it is important to conduct an After-Action Review and develop an After-Action Report (AAR) and Corrective Action Plan (CAP) to implement and track identified improvements. Additional information on AARs can be found in **Sections 3.17.8.1** and **10.2.1** of this plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK

12. PLAN DEVELOPMENT AND MAINTENANCE

12.1 PLAN DEVELOPMENT

The EOP was developed consistent with SEMS, NIMS, FEMA Comprehensive Preparedness Guide (CPG) 101, and the City's municipal code (MC § 2.52.150). The EOP guides the City's emergency management activities, and its development requires the input of all City departments.

EOP development has also been coordinated with the following plans:

- 2024 California State Emergency Plan (SEP)
- 2025 San Bernardino County Emergency Operations Plan (EOP)
- 2021 City of Redlands Local Hazard Mitigation Plan (LHMP)

This EOP is the principal reference source that guides the City's emergency management activities. Every City governmental function has a role in the EOP and, as such, shares the responsibility for input into its development and maintenance.

12.1.1 PLAN APPROVAL AND ADOPTION

Approval: There is no requirement for the City's emergency plan approval by any other level of government or external organization.

Adoption: Cal OES and FEMA require EOPs to be formally promulgated. To meet this requirement, the City will adopt the EOP by resolution of the City Council.

12.1.2 STANDARD OPERATING PROCEDURES BY DEPARTMENTS

City departments are expected to develop any policies, Standard Operating Procedures (SOPs), and Standard Operating Guidelines (SOGs) necessary to fulfill their roles and responsibilities under the EOP.

SOPs and SOGs may include the following:

- Guidance information
- Responsibilities of responding employees and agencies
- Policies and procedures
- Personnel assignments
- Contact lists

- Equipment lists
- Forms and documents

12.2 PLAN MAINTENANCE

The Director of Emergency Services has delegated the responsibility for developing, reviewing, and updating the EOP to the Fire Chief as the Emergency Manager (or designee). The EOP will be reviewed annually and comprehensively updated every five years.

Revisions, updates, and enhancements to the EOP that arise from routine improvement planning or corrective actions may be implemented without City Council adoption or additional legislative action.

Substantive changes to Part 1 of the EOP will be recorded in the Record of Changes table and digitally distributed to the departments listed in the Plan Distribution table. Non-substantive changes will not trigger redistribution.

Outdated versions should be destroyed following adoption of the current plan by City Council to ensure that only the most current version remains in circulation and to maintain compliance with the City's records retention policy.

CITY OF REDLANDS

35 CAJON ST, SUITE 200

REDLANDS, CA 92373

(909) 798-7555

APPENDIX A

RESOLUTION OF EOP ADOPTION

PURPOSE

This appendix includes the City Council resolution adopting the EOP.

RESOLUTION OF ADOPTION

[Insert the City Council resolution of adoption here.]

APPENDIX B

AUTHORITIES AND REFERENCES

This appendix establishes two foundations:

1. The legal basis—statutes, ordinances, executive orders, regulations, and proclamations—for emergency operations.
2. The basis for emergency authority, ensuring officials have the necessary powers to act during emergencies.

Not all authorities and references are used in the EOP Base Plan.

CITY OF REDLANDS

- City of Redlands Municipal Code, Chapter 2.52 – Emergency Organization

SAN BERNARDINO COUNTY

- County Resolution No. 229: California Master Mutual Aid Agreement. Adopted and approved on January 8, 1951.
- County Resolution No. 21.019 (b): Registered Volunteer Disaster Service Workers. County Code 21.0109 as repealed and reenacted through Ordinance No. 4191 related to volunteers. County Ordinance No. 4191 also includes additional information for registered disaster service workers entitlements under State law – under 21.0105 (b) (3).
- County Resolution No. 95-219: Adoption of Standardized Emergency Management System (SEMS). Adopted in September 1995, this Resolution contains language supporting the County's use and implementation of SEMS and the OA Concept.
- County Resolution No. 2006-329: Adoption of National Incident Management System (NIMS). Adopted NIMS and included language that the County would continue use of SEMS.
- County Resolution No. 21.0106: Establish Disaster Council. County Ordnance No. 4191 also defines the County's Disaster Council membership (21.0106) and powers/duties (21.0108).
- County Resolution No. 2022-222 Adoption of the 2022 Multi-Jurisdictional Hazard Mitigation Plan.

- County Resolution No. 2025-221, November 4, 2025, adopting the revised San Bernardino Emergency Operations Plan.
- County Code of Ordinances § 21.0103 establishing the Office of Emergency Services (2012).
- County Code of Ordinances § 21.0104 establishing the responsibilities and authorities of the Director of Emergency Services and the Manager of the Office of Emergency Services (2012).
- County Code of Ordinances § 21.0106 establishing the San Bernardino County Disaster Council.
- County Code of Ordinances § 21.0109 establishing the San Bernardino County Emergency Organization.

STATE OF CALIFORNIA

- California Assembly Bill 2311: Emergency Services - Access and Functional Needs (2016)
- California Constitution (Article XI: Local Government)
- California Coroners' Mutual Aid Plan
- California Disaster and Civil Defense Master Mutual Aid Agreement
- California Disaster Assistance Act (Title 19, Division 2, Chapter 6 of the California Code of Regulations)
- California Emergency Services Act (Title 2, Division 1, Chapter 7 of the Government Code)
- California Fire Service and Rescue Emergency Mutual Aid Plan
- California Government Code §3100, Disaster Service Workers and Public Employees
- California Law Enforcement Mutual Aid Plan
- California Senate Bill 160: Emergency Services - Cultural Competence (2019)
- California Assembly Bills 2311 and 477: Access and Functional Needs (2019)
- California Senate Bill 833: Emergencies - Office of Emergency Services - Guidelines - Alert and Warning Systems (2018)

- Disaster Service Worker Program Authorities (Title 1, Division 4, Chapter 8 of the Government Code and Section 3211.92 of the Labor Code)
- Standardized Emergency Management System (Title 19, Division 2, Chapter 1 of the California Code of Regulations)
- Standardized Emergency Management System Guidelines
- State of California Emergency Plan
- Title 19, Public Safety, Division 2, Chapter 2, Emergencies and Major Disasters, §2510
- Title 19, Public Safety, Division 2, Chapter 6, California Disaster Assistance Act, §2900

FEDERAL GOVERNMENT

- Americans with Disabilities Act of 1990 (PL 101-336) as amended
- Civil Rights Act of 1964 (PL 88-352, Section VI)
- Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans (2025)
- Federal Civil Defense Act of 1950 (PL 920)
- Homeland Security Act of 2002 (PL 107-296)
- Homeland Security Presidential Directive / HSPD-5: Management of Domestic Incidents
- Improving Access to Services for Persons with Limited English Proficiency (Executive Order 13166)
- Individuals with Disabilities in Emergency Preparedness (Executive Order 13347)
- National Incident Management System (updated 2017)
- National Response Framework (2019)
- Pets Evacuation and Transportation Standards Act of 2006 (PL 109-308)
- Post-Katrina Emergency Management Reform Act of 2006 (PL 109-295)
- Presidential Policy Directive / PPD-8: National Preparedness

- Robert T. Stafford Disaster Relief and Emergency Assistance Act (PL 93-288 as amended

APPENDIX C

ABBREVIATIONS AND ACRONYMS

Not all abbreviations and acronyms are used in the EOP Base Plan.

AAR/IP	After-Action Report/Improvement Plan
ADA	Americans with Disabilities Act
AHJ	Authority Having Jurisdiction
ARC	American Red Cross
Cal OES	California Governor's Office of Emergency Services
CALWAS	California Warning System
CALWARN	California Water/Wastewater Agency Response Network
CAP	Corrective Action Plan
CBO	Community Based Organization
CDAA	California Disaster Assistance Act
CERT	Community Emergency Response Team
CESFRS	California Emergency Services Fire Radio System
CESRS	California Emergency Services Radio System
CHP	California Highway Patrol
CISN	California Integrated Seismic Network
CLEMARS	California Law Enforcement Mutual Aid Radio System
CLERS	California Law Enforcement Radio System
CLETS	California Law Enforcement Telecommunications System
COG	Continuity of Government
CONFIRE	Consolidated Fire Agencies
COOP	Continuity of Operations
CPG	Comprehensive Preparedness Guide
CSTI	California Specialized Training Institute
CSWC	California State Warning Center

CUEA	California Utilities Emergency Association
DAFN	Disabilities or Access and Functional Needs
DENS	Dialogic Emergency Notification System
DHS	U.S. Department of Homeland Security
DOC	Department Operations Center
DSW	Disaster Service Worker
EAS	Emergency Alert System
EDIS	Emergency Digital Information Service
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EMMA	Emergency Managers Mutual Aid
EMSA	Emergency Medical Services Authority
ERNIE	Emergency Response Network of the Inland Empire
ESA	California Emergency Services Act
ESF	Emergency Support Function
FBO	Faith-Based Organizations
FCC	Federal Communications Commission
FCO	Federal Coordinating Officer
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FSE	Full-Scale Exercise
GIS	Geographic Information Systems
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
HUD	U.S. Department of Housing and Urban Development
IA	Individual Assistance

IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IDA	Initial Damage Assessment
IFGP	Individual and Family Grant Program
IPAWS	Integrated Public Alert and Warning System
ISO	California Independent Systems Operator
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
JPDA	Joint Preliminary Damage Assessment
JRIC	Joint Regional Intelligence Center (Los Angeles)
LEMA	Law Enforcement Mutual Aid
LHMP	Local Hazard Mitigation Plan
MAA	Mutual Aid Agreement
MACS	Multiagency Coordination System
MC	Municipal Code
MJHMP	Multi-Jurisdictional Hazard Mitigation Plan
MMAA	California Disaster and Civil Defense Master Mutual Aid Agreement
MOU	Memorandum of Understanding
NAWAS	National Warning System
NEIC	National Earthquake Information Center
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NQS	National Qualification System
NRF	National Response Framework

NRCS	Natural Resources Conservation Service
NVOAD	National Voluntary Organizations Active in Disaster
NWR	National Weather Radio
NWS	National Weather Service
OA	Operational Area
OASIS	Operational Area Satellite Information System
OES	Office of Emergency Services (San Bernardino County)
PA	Public Assistance
PETS	Pets Evacuation and Transportation Standards
PNP	Private Nonprofit Program
PPE	Personal Protective Equipment
PSEC	Public Safety Enterprise Communication
PSTN	Public Switched Telephone Network
RACES	Radio Amateur Civil Emergency Services
RAVE	Rave Mobile Safety (used by Redlands for emergency alerting)
RECG	Redlands Emergency Communications Group
REOC	Region Emergency Operations Center
RNA	Rapid Needs Assessment
SAP	Safety Assessment Program
SBA	U.S. Small Business Administration
SBCOVOAD	San Bernardino County Voluntary Organizations Active in Disaster
SCO	State Coordinating Officer
SEMS	Standardized Emergency Management System
SEP	California State Emergency Plan
SKYMARS	Sky Mutual Aid Radio System
SOC	State Operations Center
SOP	Standard Operating Procedure
TAP	Technical Assistance Programs

TDD/TTY	Telecommunications Device for the Deaf/Teletype
TENS	Telephone Emergency Notification System (San Bernardino County)
TTX	Tabletop Exercise
UC	Unified Command
USACE	U.S. Army Corps of Engineers
USGS	United States Geological Survey
VOAD	Voluntary Organizations Active in Disaster
WEA	Wireless Emergency Alerts
WRMAG	Western Region Mutual Assistance Group

APPENDIX D

GLOSSARY OF TERMS

Not all terms are used in the EOP Base Plan.

ACTION PLAN (AP): See EOC Action Plan and Incident Action Plan.

ACTIVATE: As used in this plan, shall mean the placing into operation of the Emergency Organization hereinafter provided for, upon the receipt of official warning of an impending or threatened emergency, or upon the declaration of the existence of a local emergency.

ADVISORY: According to the National Weather Service (NWS), an Advisory indicates that weather conditions that may cause inconvenience or minor impacts, requiring caution but typically not posing a significant threat to life or property.

AFTER-ACTION REPORT (AAR): A report that examines response actions, application of SEMS, modifications to plans and procedures, training needs and

recovery activities. After action reports are required under SEMS after any emergency that requires a declaration of an emergency. Reports must be submitted within 90 days to Cal OES.

AGENCY: A division of government with a specific function offering a particular kind of assistance. In the Incident Command System (ICS), agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance). Governmental organizations are most often in charge of an incident, though in certain circumstances private sector organizations may be included. Additionally, Non-Governmental Organizations (NGOs) may be included to provide support.

ALERT AND WARNING: Alert and warning refer to the systems and processes used by government agencies to notify partner organizations and the public of imminent threats or extraordinary hazards.

ANNEX: An addition to the EOP that provides specific information and direction. Appendix – Appendices provide relevant information already referenced in the guidance. Typically, this includes forms used or other necessary information.

APPENDIX: Appendices provide relevant information already referenced in the guidance. Typically, this includes forms used or other necessary information.

CALIFORNIA DISASTER AND CIVIL DEFENSE MASTER MUTUAL AID AGREEMENT (MMAA): An agreement entered into by and between the State of California, its various departments and agencies, and the various political subdivisions, municipal corporations, and public agencies of the State of California to assist each other by providing resources during an emergency. Mutual Aid occurs when two or more parties agree to furnish resources and facilities and to render services to each other in response to any type of disaster or emergency.

CALIFORNIA EMERGENCY FUNCTIONS (CA-EF): The California Emergency Functions are a grouping of state agencies, departments, and other stakeholders with similar functional activities/responsibilities whose responsibilities lend to improving the state's ability to collaboratively prepare for, effectively mitigate, cohesively respond to and rapidly recover from any emergency. California Emergency Functions unify a broad-spectrum of stakeholders with various capabilities, resources, and authorities to improve collaboration and coordination for a particular discipline. They also provide a framework for the state government to support regional and community stakeholder collaboration and coordination at all levels of government and across overlapping jurisdictional boundaries.

CALIFORNIA EMERGENCY SERVICES ACT (ESA): An Act within the California Government Code to ensure preparations within the state will be adequate to deal with natural, human-caused, or war-caused emergencies which result in conditions of disaster or in extreme peril to life, property, and the natural resources of the state, and generally to protect the health and safety and preserve the lives and property of the people of the state.

CATASTROPHE: As used in this plan, any natural or human-caused incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.

COMMAND: The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority.

COMMAND/MANAGEMENT: Command is responsible for the directing, ordering, and/or controlling of resources at the field response level. Management is responsible for overall emergency policy and coordination at the SEMS EOC levels.

COMMAND POST: See Incident Command Post.

COMMON OPERATING PICTURE: An overview of an incident created by collating and gathering information (e.g., traffic, weather, actual damage, resource availability, objectives, individual tasks, etc.) of any type (voice, data, etc.) from agencies and organizations in order to support decision making.

CONTINUITY OF GOVERNMENT (COG): As used in this plan, shall mean all measures taken to ensure the continuity of essential functions of government in the event of emergency conditions, including lines of succession for key decision makers and officials.

CONTINUITY OF OPERATIONS (COOP): As used in this plan, actions taken to ensure the continued performance of core capabilities and/or critical government operations during any potential incident.

CORRECTIVE ACTIONS: Implementing procedures that are based on lessons learned from actual incidents or from training and exercises.

CRISIS: Phenomenon, incident, active threat, or trend, with or without specific location, posing seemingly inevitable harm to life, property, environment, organizational performance, reputation, or way of life reasonably or ethically necessitating deliberate urgent intervention (A crisis may be local, national, or global)

CRITICAL INFRASTRUCTURE (CI): Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

CYBER THREAT: An act or threat that poses potentially devastating disruptions to critical infrastructure, including essential communications such as voice, email and internet connectivity.

CYBERSECURITY: The protection of data and systems in networks that are connected to the internet, including measures to protect critical infrastructure services. These services may include essential communications such as voice, email, and internet connectivity.

DAM FAILURE: Partial or complete collapse of a dam causing downstream flooding.

DEMOBILIZATION: The orderly, safe, and efficient return of an incident resource to its original location and status.

DEPARTMENT OPERATIONS CENTER (DOC): An Emergency Operations Center (EOC), specific to a single department or agency where the focus is on internal agency incident management and response.

DIRECTOR OF EMERGENCY SERVICES (DES): As used in this plan, shall mean the individual having jurisdiction and authority over a City's or County's response and recovery to extraordinary emergencies and disasters.

DISASTER: A sudden calamitous emergency event bringing great damage, loss, or destruction.

DISASTER SERVICE WORKER (DSW): As used in this plan, shall mean any person registered with a disaster council or the California Office of Emergency Services, or a state agency granted authority to register Disaster Service Workers, for the purpose of engaging in disaster service work pursuant to the California Emergency Services Act without pay or other consideration. Disaster Service Worker includes public employees, and also includes any unregistered persons impressed into service during a state of war emergency, a state of emergency, or a local emergency by a person having authority to command the aid of citizens in the execution of his or her duties.

EMERGENCY: As used in this plan, shall mean the actual or threatened existence of conditions of disaster or of extreme peril to the safety of persons and property within this city caused by such conditions as air pollution, fire, flood, storm, epidemic, riot, earthquake, drought, sudden and severe energy shortage, plant or animal infestation or disease, or other conditions, including conditions resulting from war or imminent threat of war, severe or imminent threat of terrorist attack, but other than conditions resulting from a labor controversy, which conditions are or are likely to require the combined services, personnel, equipment, and facilities of this city.

EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC): A congressionally ratified organization that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected state can request and receive assistance from other member states quickly and efficiently, resolving two key issues upfront: liability and reimbursement.

EMERGENCY OPERATIONS CENTER (EOC): As used in this plan, shall mean the physical location from which centralized city emergency management is performed. The physical location at which the coordination of information and

resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOC may be organized by major functional disciplines (e.g., fire, law enforcement and medical services), by jurisdiction (e.g., federal, state, tribal, city, county), or some combination thereof.

EMERGENCY OPERATIONS CENTER STAFF: Employees assigned to EOC functions to support the jurisdiction's response to an emergency event.

EMERGENCY OPERATIONS PLAN (EOP): The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

EMERGENCY RESPONSE AGENCY: Any organization responding to an emergency, or providing mutual aid support to such an organization, whether in the field, at the scene of an incident, or to an operations center.

EMERGENCY RESPONSE PERSONNEL: Personnel affiliated with or sponsored by emergency response agencies.

EOC ACTION PLAN (EAP): The plan developed at SEMS EOC levels, which contains objectives, actions to be taken, assignments, and supporting information for the next operational period.

ESSENTIAL FACILITIES: May include facilities such as law enforcement, fire, emergency operations centers, schools, medical facilities, and other resources that have a role in an effective and coordinated emergency response.

EVACUATION: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas and their reception and care in safe areas.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA): The Federal Emergency Management Agency (FEMA) is the federal agency responsible for coordinating emergency planning, preparedness, risk reduction, response, and recovery. The agency works closely with state and local governments by funding emergency programs and providing technical guidance and training. These coordinated activities at the federal, state, and local levels ensure a broad-based emergency program to ensure public safety and protect property.

FLOOD: A general and temporary condition of inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

FUNCTION: Function refers to the five major activities in ICS: Command, Operations, Planning, Logistics and Finance/Administration. The same five functions are also found at all SEMS EOC Levels. At the EOC, the term Management replaces Command. The term function is also used when describing the activity involved, (e.g., the planning function).

HAZARD: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

HAZARDOUS MATERIAL: Any substance or material that when involved in an accident and released in sufficient quantities poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

INABILITY TO ACT: As used in this plan, shall mean that an official is either killed, missing, or so seriously ill or injured as to be unable to attend meetings and otherwise perform his/her duties. Any question as to whether a particular official can be deemed to have an "inability to act" shall be settled by the governing board of the political jurisdiction or any remaining available members of said body (including standby officers who are serving on such body).

INCIDENT: An occurrence or event, natural or human-caused, which requires a response to protect life or property.

INCIDENT ACTION PLAN (IAP): An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods. At the SEMS EOC level it is called the EOC Action Plan.

INCIDENT COMMAND (IC): Responsible for overall management of the incident and consists of the Incident Commander, either single or unified command, and any assigned supporting staff. Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics, and

the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

INCIDENT COMMAND POST (ICP): The field location where the primary functions are performed. The ICP may be co-located with the incident base or other incident facilities.

INCIDENT COMMAND SYSTEM (ICS): A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

INTELLIGENCE: Product of an analytical process that evaluates information collected from diverse sources; integrates the relevant information into a cohesive package and produces a conclusion or estimate. Information must be real, accurate and verified before it becomes intelligence for planning purposes. Intelligence relates to the specific details involving the activities of an incident or EOC and current and expected conditions and how they affect the actions taken to achieve operational period objectives. Intelligence is an aspect of information. Intelligence is primarily intended for internal use and not for public dissemination.

INTEROPERABILITY: Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real-time, when needed and when authorized.

JOINT INFORMATION CENTER (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media. Public information officials from all participating agencies should co-locate at the JIC.

JOINT INFORMATION SYSTEM (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing,

recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.

JURISDICTION: A range or sphere of authority. Public agencies have jurisdiction over an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., federal, state, tribal, and local boundary lines) or functional (e.g., law enforcement, public health).

KEY RESOURCES: Any publicly or privately controlled resources essential to the minimal operations of the economy and government.

LIAISON: A form of communication for establishing and maintaining mutual understanding and cooperation.

LOCAL EMERGENCY: As used in this plan, shall mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the territorial limits of a county, city and county, or city, caused by such conditions as air pollution, fire, flood, storm, epidemic, pandemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, including conditions resulting from war or imminent threat of war, severe or imminent threat of terrorist attack, other than conditions resulting from a labor controversy, which conditions are or are likely to be beyond the control of the services, personnel, equipment, and facilities of that political subdivision and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the State Public Utilities Commission.

LOCAL GOVERNMENT: According to Federal Code 30 a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal entity, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity.

MITIGATION: Provides a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect.

MOBILIZATION: The process and procedures used by all organizations - federal, state, tribal, and local - for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.

MOBILIZATION CENTER: An off-emergency location where emergency services personnel and equipment may be temporarily located, pending assignment to emergencies, released, or reassigned.

MULTI-AGENCY OR INTER-AGENCY COORDINATION (MAC): The participation of agencies and disciplines involved at any level of the SEMS organization working together in a coordinated effort to facilitate decisions for overall emergency response activities, including the sharing of critical resources and the prioritization of incidents.

MULTI-AGENCY COORDINATION GROUP (MAC GROUP): Typically, administrators/executives, or their appointed representatives, who are authorized to commit agency resources and funds, are brought together and form MAC Groups. MAC Groups may also be known as multi-agency committees, emergency management committees, or as otherwise defined. It can provide coordinated decision-making and resource allocation among cooperating agencies and may establish the priorities among incidents, harmonize agency policies, and provide strategic guidance and direction to support incident management activities.

MULTI-AGENCY COORDINATION SYSTEM(S) (MACS): Multi-agency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The elements of multi-agency coordination systems include facilities, equipment, personnel, procedures, and communications. Two of the most commonly used elements are EOC and MAC Groups. These systems assist agencies and organizations responding to an incident.

MUTUAL AID AGREEMENTS AND/OR ASSISTANCE AGREEMENTS: Written or oral agreements between and among agencies/or organizations and/or jurisdictions

that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

MUTUAL AID COORDINATOR: An individual at the local government, operational area, region, or state level that is responsible to coordinate the process of requesting, obtaining, processing, and using mutual aid resources. Mutual Aid Coordinator duties will vary depending upon the mutual aid system.

MUTUAL AID REGION: A mutual aid region is a subdivision of Cal OES established to assist in the coordination of mutual aid and other emergency operations within a geographical area of the state, consisting of two or more operational areas.

MULTI-AGENCY OR INTER-AGENCY COORDINATION: As used in this plan, it shall mean the participation of agencies and disciplines involved at any level of the Standardized Emergency Management System (SEMS) organization working together in a coordinated effort to facilitate decisions for overall emergency response activities, including the sharing of critical resources and the prioritization of incidents.

NATIONAL: Of a nationwide character, including the federal, state, tribal and local aspects of governance and policy.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS): As used in this plan, it shall mean the adopted national emergency management processes, protocols, and procedures for federal, state, tribal and local responders. National Incident Management System (NIMS) utilizes the Incident Command System (ICS), Resource Management, Joint Information Management System, Communication and Information Management and Preparedness policies. NIMS is consistent with SEMS.

NATIONAL RESPONSE FRAMEWORK (NRF): A guide to how the nation conducts all-hazards incident management.

NATURAL DISASTER: Any hurricane, tornado, storm, flood, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, drought, fire, or other catastrophe which causes, or which may cause, substantial damage or injury to civilian property or persons**.**

NON-GOVERNMENTAL ORGANIZATION (NGO): An entity with an association based on the interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with the government. Such organizations serve a public purpose, not a private benefit. Examples of NGO include faith-based charity organizations and the American Red Cross.

OPERATIONAL AREA (OA): As used in this plan, it shall mean an intermediate level of state emergency services organization, consisting of a county and all political subdivisions within the county area. Each county geographic area is designated an operational area for the coordination of emergency activities and to serve as a link in the system of communications and coordination between the state's emergency operations centers and the operations centers of the political subdivisions comprising the operational area, as defined in California Government Code Subsection 8559 (b) and Section 8605. This definition does not change the definition of operational area as used in the existing fire and rescue mutual aid system.

OPERATIONAL AREA EMERGENCY OPERATIONS CENTER (OA EOC): The physical location at which the coordination of information and resources to support OA activities normally takes place.

OPERATIONAL PERIOD: The time scheduled for executing a given set of operation actions, as specified in the Incident Action Plan or EOC Action Plan. Operational periods can be of various lengths, although usually last 12-24 hours.

ORGANIZATION: Any association or group of persons with like objectives. Examples include, but are not limited to, governmental departments and agencies, private sector, and/or non- governmental organizations.

OUTLOOK: According to the National Weather Service (NWS), an Outlook indicates the potential for hazardous weather over the coming days, intended to provide advance awareness with low certainty and no immediate action required.

PLAN: A document that describes the broad, overall jurisdictional response to potential extraordinary emergencies or disasters.

POLITICAL SUBDIVISIONS: Includes any city, city and County, County, tax or assessment district, or other legally authorized local governmental entity with jurisdictional boundaries.

PREPAREDNESS: A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response. Within NIMS, preparedness focuses on the following elements: planning, procedures and protocols, training and exercises, personnel qualification and certification, and equipment certification.

PREVENTION: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice.

PRIVATE SECTOR: Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry.

PROTOCOLS: Sets of established guidelines for actions (which may be designated by individuals, teams, functions, or capabilities) under various specified conditions.

PUBLIC INFORMATION: Processes, procedures, and systems for communicating timely, accurate and accessible information on the incident's cause, size and current situation; resources committed; and other matters of general interest to the public, responders and additional stakeholders (both directly affected and indirectly affected).

PUBLIC INFORMATION OFFICER (PIO): A member of the Command Staff (Management Staff at the SEMS EOC Levels) responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements.

RECOVERY: The development, coordination, and execution of service and site restoration plans; the reconstitution of government operations and services; individual, private sector, non-governmental, and public assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and

economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

RECOVERY PLAN: A plan developed to restore the affected area or community.

REGION EMERGENCY OPERATIONS CENTER (REOC): Facilities found at Cal OES Administrative Regions. REOC provides centralized coordination of resources among Operational Areas within their respective regions and between the Operational Areas and the State Level.

REIMBURSEMENT: Provides a mechanism to recoup funds expended for incident-specific activities.

RESOURCE MANAGEMENT: Efficient emergency management and incident response requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under NIMS includes mutual aid agreements and assistance agreements; the use of special federal, state, tribal and local teams; and resource mobilization protocols.

RESOURCES: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.

RESPONSE: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of EOP and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

RESPONSE PERSONNEL: Includes federal, state, territorial, tribal, sub-state regional and local governments, private sector organizations, critical infrastructure owners and operators, NGO and all other organizations and individuals who assume an emergency management role. Also known as an Emergency Responder.

SITUATION REPORT: Often contains confirmed or verified information regarding the specific details relating to the incident.

SPAN OF CONTROL: The number of resources for which a supervisor is responsible, usually expressed as the ratio of supervisors to individuals. Under NIMS, an appropriate span of control is between 1:3 and 1:7, with optimal being 1:5.

SPECIAL DISTRICT: A unit of local government (other than a city, county, or city and County) with authority or responsibility to own, operate and maintain systems, programs, services, or projects (as defined in California Code of Regulations (CCR) Section 2900(s) for purposes of natural disaster assistance. This may include a joint power authority established under Section 6500 et. seq. of the Code.

STAFFORD ACT: The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) establishes the programs and processes for the federal government to provide disaster and emergency assistance to states, local governments, tribal nations, individuals, and qualified private nonprofit organizations. The provisions of the Stafford Act cover all hazards including natural disasters and terrorist events. Relevant provisions of the President. The President may declare a major disaster or emergency.

STAGING AREA: Established on an incident for the temporary location of available resources. A Staging Area can be any location on an incident in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment.

STANDARD OPERATING PROCEDURE/GUIDE (SOP/SOG): Complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS): As used in this plan shall mean the adopted State of California emergency management system. The Standardized Emergency Management System (SEMS) utilizes the Incident Command System (ICS), Multi/Interagency Coordination, Mutual Aid, and the

Operational Area Concept to facilitate emergency incident management, priority setting, interagency cooperation, and the efficient use of resources and flow of information during an emergency. SEMS is consistent with NIMS.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS) GUIDELINES: The SEMS guidelines are intended to assist those responsible for planning, implementing, and participating in SEMS.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS) REGULATIONS: Regulations establishing the Standardized Emergency Management System (SEMS) based upon the Incident Command System (ICS) adapted from the system originally developed by the Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE) program including those currently in use by state agencies, the Multiagency Coordination System (MACS) as developed by FIRESCOPE program, the Operational Area concept and the Master Mutual Aid Agreement and related mutual aid systems. Regulations are found in TITLE 19. DIVISION 2. Chapter 1, Section 2400 et. Seq.

STATE: When capitalized, refers to any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. See Section 2 (14), Homeland Security Act of 2002, Public Law 107−296, 116 Stat. 2135 (2002).

STATEMENT: According to the National Weather Service (NWS), a Statement provides additional information, updates, or clarification about ongoing or recent weather conditions.

STATE OF EMERGENCY: As used in this plan, shall mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the state caused by such conditions as air pollution, fire, flood, storm, epidemic, pandemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, other than conditions resulting from a labor controversy or conditions causing a state of war emergency, which conditions, by reason of their magnitude, are or are likely to be beyond the control of the services, personnel, equipment, and facilities of any single county, city and county, or city and require the combined forces of a mutual aid region or regions to combat, or with respect to regulated energy utilities, a sudden and

severe energy shortage requires extraordinary measures beyond the authority vested in the State Public Utilities Commission.

STATE OF WAR EMERGENCY: As used in this plan, shall mean the condition which exists immediately, with or without a proclamation thereof by the Governor, whenever this state or nation is attacked by an enemy of the United States, or upon receipt by the state of a warning from the federal government indicating that such an enemy attack is probable or imminent.

STATE OPERATIONS CENTER (SOC): The SOC is operated by the California Governor's Office of Emergency Services (Cal OES)at the State Level in SEMS. It is responsible for centralized coordination of state resources in support of the three Cal OES Administrative Regional Emergency Operations Centers (REOCs). It is also responsible for providing updated situation reports to the Governor and legislature.

SYSTEM: An integrated combination of people, equipment and processes that work in a coordinated manner to achieve a specific desired output under specific conditions.

TECHNICAL ASSISTANCE: Support provided to state, tribal and local jurisdictions when they have the resources but lack the complete knowledge and skills needed to perform the required activity (such as mobile-home park design or hazardous material assessments).

TECHNICAL SPECIALISTS: Personnel with special skills that can be used anywhere within the SEMS organization. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically certified in their fields or professions.

TERRORISM: Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any state or other subdivision of the United States in which it occurs; and is intended to intimidate or coerce the civilian population, or influence or affect the conduct of a government by mass destruction, assassination, or kidnapping.

THREAT: An indication of possible violence, harm, or danger.

TYPE: 1) An ICS resource classification that refers to capability. Type 1 is generally considered to be more capable than Types 2, 3, or 4, respectively, because of size, power, capacity, or (in the case of incident management teams) experience and qualifications. 2) A class, kind, or group sharing one or more characteristics; category. 3) A variety or style of a particular class or kind of things.

UNIFIED COMMAND (UC): An ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.

VITAL RECORDS: The essential agency records needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records), or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

VOLUNTEER: As used in this plan, a volunteer is any individual accepted to perform services by the lead agency (which has authority to accept volunteer services) when the individual performs services without promise, expectation, or receipt of compensation for services performed. A volunteer may be “affiliated” with a volunteer organization or may be “spontaneous unaffiliated” when pressed into volunteer service at the time of a disaster.

WARNING: According to the National Weather Service (NWS), a Warning indicates that a hazardous event is imminent or occurring, requiring immediate protective action.

WATCH: According to the National Weather Service (NWS), a Watch indicates that conditions are favorable for a specific hazard to develop, meaning individuals should remain alert and prepared to take action.

WebEOC: A cloud-based emergency management and continuity platform by Juvare that enables organizations to maintain a common operating picture and coordinate information, resources, and workflows during incidents and daily operations.

APPENDIX E

EOC STAFFING MATRIX

Each EOC function is assigned to one or more City department or contract agency.

EOC STAFFING MATRIX FOR CITY DEPARTMENTS	
MANAGEMENT SECTION	
POSITION	**FILLED BY**
EOC Director	City Manager's Office
EOC Coordinator	Fire Department
Liaison Officer	City Clerk's Office
Public Information Officer	Communications and Community Relations Office
Safety Officer	Human Resources Department
Security Officer	Police Department, or Call-When-Needed Contract Security Company
Legal Advisor	City Attorney
OPERATIONS SECTION	
POSITION	**FILLED BY**
Operations Section Chief	TBD – Incident Specific
Fire & Rescue Branch Director	Fire Department
Law Enforcement Branch Director	Police Department
Facilities and Community Services Branch Director	Facilities and Community Services Department
Utilities Branch Director	Municipal Utilities and Engineering Department

PLANNING & INTELLIGENCE SECTION	
POSITION	**FILLED BY**
Planning & Intelligence Section Chief	Development Services Department
Situation Analysis Unit Leader	Development Services Department (Planning Division)
Advanced Planning Unit Leader	Development Services Department
Documentation Unit Leader	Development Services Department
GIS Unit	Management Services (GIS Division)
Demobilization Unit Leader	Facilities and Community Services Department
Technical Specialists	TBD – Incident Specific
LOGISTICS SECTION	
POSITION	**FILLED BY**
Logistics Section Chief	Facilities and Community Services Department
Communications Unit Leader	Management Services (Innovation & Technology Division)
Facilities Unit Leader	Facilities and Community Services Department
Food Unit Leader	Facilities and Community Services Department
Human Resources Unit Leader	Human Resources Department
Information Technology Unit Leader	Management Services (Innovation & Technology Division)
Medical Unit Leader	Fire Department
Supply & Procurement Unit Leader	Management Services (Finance Division)
Volunteer Management Unit Leader	Human Resources Department

FINANCE & ADMINISTRATION SECTION	
POSITION	**FILLED BY**
Finance and Administration Section Chief	Management Services (Finance Division)
Compensation & Claims Unit Leader	Management Services (Finance Division)
Cost Analysis Unit Leader	Management Services (Finance Division)
Cost Recovery Unit Leader	Management Services (Finance Division)
Time Keeping Unit Leader	Management Services (Finance Division)

APPENDIX F

EMERGENCY SUPPORT FUNCTIONS CROSSWALK

The table below presents the San Bernardino County, State, and Federal Emergency Support Functions (ESF).

EMERGENCY SUPPORT FUNCTIONS		
SAN BERNARDINO COUNTY ESF	**CALIFORNIA ESF**	**FEDERAL ESF**
ESF-1 Transportation	ESF-1 Transportation	ESF-1 Transportation
ESF-2 Communications	ESF-2 Communications	ESF-2 Communications
ESF-3 Construction and Engineering	ESF-3 Construction and Engineering	ESF-3 Public Works and Engineering
ESF-4 Firefighting and Rescue	ESF-4 Fire and Rescue	ESF-4 Firefighting
ESF-5 Emergency Management	ESF-5 Management	ESF-5 Information and Planning
ESF-6 Mass Care, Sheltering, and Human Services	ESF-6 Mass Care and Shelter	ESF-6 Mass Care, Emergency Assistance, Temporary Housing, and Human Services
ESF-7 Logistics and Resource Support	ESF-7 Resources	ESF-7 Logistics
ESF-8 Public Health and Medical	ESF-8 Public Health and Medical	ESF-8 Public Health and Medical Services
ESF-9 Search and Rescue	ESF-9 Search and Rescue	ESF-9 Search and Rescue

ESF-10 Hazardous Materials	ESF-10 Hazardous Materials	ESF-10 Oil and Hazardous Materials Response
ESF-11 Food and Agriculture	ESF-11 Food and Agriculture	ESF-11 Agriculture and Natural Resources
ESF-12 Energy and Utilities	ESF-12 Utilities	ESF-12 Energy
ESF-13 Public Safety, Law Enforcement, and Security	ESF-13 Law Enforcement	ESF-13 Public Safety and Security
ESF-14 Long-Term Community Recovery	ESF-14 Recovery	ESF-14 Cross-Sector Business and Infrastructure
ESF-15 Public Information	ESF-15 Public Information	ESF-15 External Affairs
ESF-16 Evacuation and Re-Entry	ESF-16 Evacuation	
ESF-17 Volunteer and Donations Management	ESF-17 Volunteer and Donations Management	
ESF-18 Cybersecurity	ESF-18 Cybersecurity	
ESF-19 Debris Management		
ESF-20 Commodities Distribution		
ESF-21 Alert and Warning		

RESOLUTION NO. 6888

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS ADOPTING THE CITY OF REDLANDS' EMERGENCY OPERATIONS PLAN

WHEREAS, the City of Redlands is subject to earthquake, fire, flood, terrorism and other serious hazards; and

WHEREAS, the overall objective of emergency management for the City of Redlands is to ensure the effective management of response forces and resources in preparing for and responding to situations associated with natural disaster, technological incidents and nation security emergencies; and

WHEREAS, the City of Redlands' emergency management is committed to provide effective life safety measures while reducing property loss and damage to the environment and provide for rapid resumption of impacted businesses and community services; and

WHEREAS, the City of Redlands is primarily responsible for emergency actions and will commit all available resources to save lives, minimize injury to persons and minimize damage to property and the environment; and

WHEREAS, the City of Redlands has implemented the Standardizes Emergency Management System as required by section 8607 of the California Emergency Services Act; and,

WHEREAS, the City of Redlands' Emergency Operations Plan serves as a basis for effective response to any hazard that threatens the City of Redlands; and

WHEREAS, the City of Redlands' Emergency Operations Plan serves as a legal and conceptual framework for emergency management in the City of Redlands,

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Redlands, hereby adopts the City of Redlands' Emergency Operations Plan dated September 15, 2009, on file in the office of the City Clerk.

ADOPTED, SIGNED AND APPROVED THIS 15th day of September 2009.

Jon Harrison, Mayor of the City of Redlands

ATTEST:

Lorrie Poyzer, City Clerk

I, Lorrie Poyzer, City Clerk of the City of Redlands, hereby certify that the foregoing Resolution was duly adopted by the City Council at a regular meeting thereof, held on the 15th day of September, 2009, by the following vote:

AYES: Councilmembers Gallagher, Aguilar, Bean; Mayor Harrison
NOES: None
ABSENT: Councilmember Gilbreath
ABSTAIN: None

Lorrie Poyzer, City Clerk
City of Redlans, California

EMERGENCY OPERATIONS PLAN

A STRATEGY FOR THE CITYWIDE RESPONSE TO MAJOR EMERGENCIES AND DISASTERS

JULY 2026

Portions of the Emergency Operations Plan, including supporting parts and annexes, may contain sensitive information related to the deployment, mobilization, and tactical operations of the City of Redlands government and cooperating or assisting agencies in response to emergencies.

While the EOP Base Plan (Part 1) is available for public use and review, the City may withhold certain supporting parts and annexes from full public disclosure under the provisions of the California Public Records Act (California Government Code § 7920-7931).

PROMULGATION STATEMENT

This **Emergency Operations Plan** is adopted as the official emergency plan of the City of Redlands by Resolution No. 8827 of the City of Redlands City Council, California, dated October 6, 2026. This version supersedes all previous versions.

_____

MARIO SAUCEDO, MAYOR

City of Redlands

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Preface **9**

Concurrence Signatures to the Emergency Operations Plan **17**

Plan Organization and Activation **19**

Plan Organization 19

Plan Activation 19

Triggering Events 20

Preemptive Response Actions 20

How to Use This Plan 21

1. Purpose and Scope **23**

1.1 Purpose 23

1.2 Scope 23

1.3 Basis for Planning 24

1.4 Response Objectives 24

2. Situation and Assumptions **25**

2.1 Situation Overview 25

2.2 Hazards Summary 26

2.3 Planning Assumptions 28

3. Concept of Operations **29**

3.1 General Overview 29

3.2 Phases of Emergency Management 29

3.3 Standardized Emergency Management System 34

3.4 National Incident Management System 36

3.5 Incident Command System 36

3.6 Emergency Support Functions 37

3.7 Emergency Proclamations 37

3.8 Operating Conditions 39

3.9 EOC Activation and Deactivation 41

3.10 EOC Activation Levels 43

3.11 EOC Staffing Matrix for City Departments 47

3.12 EOC Action Plans....47
3.13 Cultural Competence....48
3.14 Disabilities or Access and Functional Needs Populations....48
3.15 Animal Care Considerations....49
3.16 Recovery Organization....50
3.17 Recovery Operations....50
3.18 Emergency Facilities....59
4. Organization and Assignment of Responsibilities....63
4.1 City Level....63
4.2 Operational Area Level....66
4.3 Regional Level....67
4.4 State Level....67
4.5 Federal Level....67
4.6 External Partners....68
5. Direction, Control, and Coordination....73
5.1 Director of Emergency Services....73
5.2 City EOC....73
5.3 City Department Direction....73
5.4 Department Operations centers....73
5.5 Local Control....73
5.6 On-Scene Control....74
5.7 Coordination and Interface....74
6. Information Collection, Analysis, and Dissemination....79
6.1 Objectives....79
6.2 Information Collection....80
6.3 Analysis and Dissemination....82
7. Communications....85
7.1 Public Alert and Warning....85
7.2 Communication Systems....90
7.3 Public Information....93

8. Mutual Aid and Resource Management 95
8.1 Mutual Aid Overview 95
8.2 Mutual Aid Agreements 95
8.3 California Mutual Aid Framework 96
8.4 City Mutual Aid Participation 100
8.5 Emergency Management Assistance Compact 102
8.6 Resource Management Overview 103
9. Continuity of Government 107
9.1 Reconstitution of Government 107
9.2 Director of Emergency Services 108
9.3 Succession of Officers 109
9.4 Alternate Seat of Government 110
9.5 Preservation of Vital Records 110
10. Administration, Finance, and Logistics 113
10.1 Administrative Practices 113
10.2 Documentation 113
10.3 Finance During Disasters 114
10.4 Logistics 115
11. Training and Exercise 117
11.1 Emergency Operations Training 117
11.2 Emergency Operations Exercises 118
12. Plan Development and Maintenance 121
12.1 Plan Development 121
12.2 Plan Maintenance 122

Appendices

Appendix A: Resolution of EOP Adoption
Appendix B: Authorities and References
Appendix C: Abbreviations and Acronyms
Appendix D: Glossary of Terms
Appendix E: EOC Staffing Matrix
Appendix F: Emergency Support Functions Crosswalk

THIS PAGE IS INTENTIONALLY LEFT BLANK

PREFACE

EOP OVERVIEW

The City of Redlands Emergency Operations Plan (EOP) outlines the concepts and strategies used to prevent, mitigate, prepare for, protect against, respond to, and recover from natural, technological, and human-caused hazards that could impact the City. All actions described in the EOP are focused on protecting life, property, and the environment; maintaining essential government operations; and supporting a timely transition to recovery. The EOP is developed with an emphasis on coordination, collaboration, and cooperation.

EOP DEVELOPMENT

The EOP has been developed in accordance with the California Standardized Emergency Management System (SEMS) and the National Incident Management System (NIMS). The EOP is written in coordination with the State of California Emergency Plan, the National Response Framework, and FEMA's "Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans".

The City of Redlands the Disaster Council is responsible for developing "emergency and mutual aid plans and agreements" (City of Redlands Municipal Code (MC) MC § 2.52.060). The Emergency Plan (MC § 2.52.150) is developed to "provide for the effective mobilization of all of the resources of the City, both public and private, to meet any condition constituting a local emergency, state of emergency, or state of war emergency."

The City Manager, as the Director of Emergency Services, is empowered to "control and direct the effort of the emergency organization of the City" (MC § 2.52.100) and is ultimately responsible for directing disaster readiness, emergency planning, and response and recovery efforts.

This plan provides the framework within which City departments, special districts, allied agencies, non-governmental organizations, volunteer groups, and private organizations can develop detailed response procedures, continuity of government/continuity of operations plans, resource arrangements, and aid agreements. These departments, agencies, and organizations collectively comprise the City of Redlands Emergency Organization (MC § 2.52.140).

EOP ORGANIZATION

To ensure the greatest flexibility, the EOP is organized in parts focusing on specific emergency management areas. City departments may develop and maintain standard operating procedures (SOPs) as needed to support their role in the EOP.

The EOP consists of five parts:

1. Part 1: Base Plan
2. Part 2: Emergency Operations Center (EOC) Position Checklists
3. Part 3: Functional Annexes
4. Part 4: Hazard-Specific Annexes
5. Part 5: Supporting Attachments

While some parts of the EOP are complete, others may be under development, in the revision process, or scheduled for future planning efforts.

EOP SUPPORTING PROCEDURES

Recipients of this EOP are responsible for developing detailed plans, procedures, agreements, and arrangements specific to their departments or agencies. They must ensure personnel are trained to implement these measures and make updates as needed. Departments or agencies assigned responsibilities under this plan should have access to the emergency resources identified in the plan, as well as the ability to obtain those resources during an emergency or disaster.

EOP UPDATES

Emergency planning is a continuous, cyclical process and the EOP will be regularly reviewed and updated to reflect changes. Revisions may be made based on lessons learned from real-world incidents and exercises; advancements in technology; new laws or regulations; organizational changes within the jurisdiction; and shifts in local or partner agency capabilities. The City will issue supplements to this plan as needed to address specific hazards, specialized emergency functions, or complex planning issues. Regular and routine updates may be made without further promulgation or legislative action.

SUMMARY

While no plan can fully prevent the loss of life or damage to property, well-developed plans carried out by trained and knowledgeable personnel can help minimize these losses. City departments, allied agencies, non-governmental organizations, volunteer groups, and private entities are encouraged to take all necessary preparedness actions to fulfill their roles in the EOP.

THIS PAGE IS INTENTIONALLY LEFT BLANK

RECORD OF CHANGES

DATE	CHANGE NO.	PART, ANNEX, OR ATTACHMENT CHANGED	PERSON MAKING CHANGE

THIS PAGE IS INTENTIONALLY LEFT BLANK

PLAN DISTRIBUTION	
DEPARTMENT / AGENCY / ORGANIZATION	
City of Redlands City Manager's Office	City of Redlands City Attorney's Office
City of Redlands City Clerk's Office	City of Redlands Fire Department
City of Redlands Management Services/Finance Department	City of Redlands Police Department
City of Redlands Human Resources Department	City of Redlands Municipal Utilities & Engineering Department
City of Redlands Facilities & Community Services Department	City of Redlands Development Services Department
City of Redlands EOC (Primary)	City of Redlands Library
City of Redlands EOC (Alternate)	

DISTRIBUTION METHODOLOGY

- All planning documents will be distributed digitally.
- Part 1 Base Plan will be distributed upon promulgation.
- All other EOP components—including attachments, annexes, and appendices—will be distributed as they are developed, updated, or revised.

THIS PAGE IS INTENTIONALLY LEFT BLANK

CONCURRENCE SIGNATURES TO THE EMERGENCY OPERATIONS PLAN

City Manager/Director of Emergency Services

Assistant City Manager

Assistant City Manager

City Attorney

City Clerk

Fire Chief

Police Chief

Director, Management Services/Finance Department

Director, Municipal Utilities & Engineering Department

Director, Human Resources Department

Director, Facilities & Community Services Department

Director, Development Services Department

Director, Library

Concurrence indicates agreement with
the general concept of operations of the plan
and department, agency, or organization assigned tasks.

THIS PAGE IS INTENTIONALLY LEFT BLANK

PLAN ORGANIZATION AND ACTIVATION

PLAN ORGANIZATION

The EOP is divided into five distinct parts to enhance its usability and flexibility for emergency personnel and key City officials.

PART 1: BASE PLAN

Authorities, concept of operations, and assignment of responsibilities.

PART 2: EOC POSITION CHECKLISTS

EOC activation procedures, organization, and functional position descriptions.

PART 3: FUNCTIONAL ANNEXES

Standard operating concepts and procedures for commonly required EOC emergency response and support functions.

PART 4: HAZARD-SPECIFIC ANNEXES

Standard operating concepts and procedures that are unique to specific hazards and threats.

PART 5: SUPPORTING ATTACHMENTS

Reserved for supporting documents and references essential to the execution of the jurisdictional EOP and not fitting into Parts 2-4.

While some parts of the EOP are complete, others may be under development, in the revision process, or scheduled for future planning efforts.

PLAN ACTIVATION

The plan will become activated:

- By order of the City Manager as the Director of Emergency Services, or the Assistant City Manager, or the Fire Chief, or the Chief of Police, or a Department Director, or a designee, or
- Upon the proclamation of a local emergency or when conditions exist that may warrant such a proclamation, consistent with the authority granted in MC § 2.52.100, or

- When the Governor has proclaimed a State of Emergency in an area, including the City of Redlands, or
- At the proclamation of a State of War Emergency, as defined by the California Emergency Services Act, or
- Upon a Triggering Event identified within this section.

In the event of a threatened emergency, all or part of the City's Emergency Organization (MC § 2.52.140) may be mobilized—even before this plan is formally activated—by order of the City Manager, Assistant City Manager, Fire Chief, Chief of Police, a Department Director, or a designee.

TRIGGERING EVENTS

The following events may trigger the activation of the EOP and EOC:

- Damaging earthquake, wildfire, flood, or other impactful event
- Severe weather warning
- Significant commitment or draw-down of City emergency resources
- Regularly scheduled emergency exercises or training activities
- City-sponsored special events of extraordinary significance
- Any incident that inhibits the City's ability to deliver essential services
- Any situation in which City resources are overwhelmed, and a coordinated response is required to protect life, property, or public safety

PREEMPTIVE RESPONSE ACTIONS

Prior to a potential, impending, or threatened emergency, actions will be taken to prevent an incident, reduce its impact, or enhance City readiness. These actions may include but are not limited to gathering and maintaining situational awareness and resource status information; pre-alerting response departments and partner organizations; developing incident-specific contingency plans and staffing strategies; pre-positioning response assets and emergency supplies; and establishing and maintaining communication with Department Directors, assisting and cooperating agencies, and the City's Emergency Organization.

Preemptive response actions may be ordered by the City Manager, Assistant City Manager, Fire Chief, Chief of Police, a Department Director, or a designee.

HOW TO USE THIS PLAN

Prior to EOP Activation

- Understand departmental or organizational responsibilities
- Develop all necessary supporting Standard Operating Procedures (SOPs)
- Acquire and allocate resources necessary to fulfill assigned responsibilities
- Train staff and teams to perform their roles as outlined in the EOP or SOPs

Upon EOP Activation

- Refer to the EOC organizational chart in EOP Part 2 (Position Checklists)
- Identify the function for which your department or organization is responsible and ensure it is staffed within the City's EOC
- Locate the corresponding section in EOP Part 2 that outlines the function and associated tasks
- Under the direction of the Director of Emergency Services/EOC Director, carry out the functions and associated tasks consistent with the EOC Action Plan or stated incident priorities

THIS PAGE IS INTENTIONALLY LEFT BLANK

1. PURPOSE AND SCOPE

1.1 PURPOSE

This plan outlines the actions to be taken by the City to prevent disasters where possible, reduce vulnerability, protect people and property, respond effectively, and recover from extraordinary emergencies and disasters.

The Emergency Operations Plan (EOP) serves as the primary guide for the City's Emergency Organization, outlining procedures to effectively plan, prepare for, and respond to emergencies.

1.2 SCOPE

The City's EOP uses an all-hazards approach to outline its planned response to extraordinary emergencies caused by natural disasters and human-caused incidents. While it does not address routine, day-to-day emergencies, the plan focuses on large-scale disasters and catastrophic incidents that may create unique situations requiring a significant response. The Base Plan establishes authority and provides a foundational concept of operations upon which further plans, procedures, guidelines, arrangements, and agreements can be built.

The EOP is designed to be adaptable, supporting any emergency or disaster affecting the City. It prioritizes initial response efforts on saving lives, protecting property, and meeting basic human needs in the immediate aftermath of an emergency or disaster. Additionally, the plan guides the restoration of affected areas to normalcy and helps mitigate further harm or damage during recovery efforts.

The EOP applies to all City departments and external entities that may assist in an emergency or disaster. Departments can respond within their own authorities and capabilities or as part of a coordinated citywide effort. References to City departments include divisions and organizational units, while non-governmental and quasi-governmental organizations (e.g., school districts, telecommunications providers, universities, and volunteer groups) may also play a supporting role in response and recovery efforts.

1.3 BASIS FOR PLANNING

California Government Code § 8568 states: "The State Emergency Plan shall be in effect in each political subdivision of the state, and the governing body of each political subdivision shall take such action as may be necessary to carry out the provisions thereof."

United States Homeland Security Presidential Directive-5 (HSPD-5) directs the development and implementation of the National Incident Management System (NIMS). NIMS requires developing and maintaining various planning elements at the local government level, including the EOP.

The City EOP is developed in accordance with the MC § 2.52.150 and takes effect upon adoption by resolution of the City Council.

1.4 RESPONSE OBJECTIVES

The following objectives guide the planning and the conduct of response and recovery efforts for the City during an emergency:

- Protect lives
- Provide for the continuity of government
- Safeguard property, the environment, and the economy
- Repair and restore essential systems, services, and lifelines
- Provide a basis for direction and control of emergency operations
- Provide for the protection, use, and distribution of emergency resources
- Coordinate emergency operations with other jurisdictions and emergency service organizations.

2. SITUATION AND ASSUMPTIONS

2.1 SITUATION OVERVIEW

History: Redlands was incorporated in 1888 after attracting eastern and midwestern settlers who shaped it into a cultural, educational, and agricultural community. Founded by Frank E. Brown and E. G. Judson, the City grew around citrus—especially the Washington navel orange—earning recognition as the "Navel Orange Capital of the World." Philanthropic leaders including Alfred H. and Albert K. Smiley, Clarence G. White, and Robert Watchorn established lasting cultural landmarks, reinforcing Redlands' reputation as the "Jewel of the Inland Empire." The City prospered through the early 20th century with citrus agriculture, the University of Redlands, and Norton Air Force Base, though the base's 1994 closure and the economic downturn beginning in 1990 challenged its stability.

Location: Redlands is located in San Bernardino County within Southern California's Inland Empire, positioned at the base of the San Bernardino Mountains. The City is located approximately 63 miles east of Los Angeles and spans 36.25 square miles. Redlands shares borders with the communities of Highland, Mentone, Crafton, Yucaipa, Loma Linda, and portions of San Bernardino. Its elevation averages 1,358 feet above sea level, placing it at a natural transition zone between the urbanized Inland Empire and the mountain and desert corridors to the east.

Climate: The City has a Mediterranean climate, characterized by mild, wet winters and warm, dry summers. Temperatures are generally moderate to warm throughout the year, with average highs ranging from 67°F in winter to 96°F in summer. The City averages 12.9 inches of rainfall per year.

Demographics: According to 2025 U.S. Census estimates, the City's population is approximately 74,128. The three largest racial/ethnic demographic groups in the City are White (47.9%), Hispanic/Latino (39.5%), and Asian (8.6%). Approximately 30.1% of the population speaks a language other than English at home.

City Services: The City of Redlands is a general law city operating under a council-manager form of government. The City provides its own police and fire protection services through the Redlands Police Department and the Redlands Fire Department. The City also operates a general aviation airport, maintains a municipal animal shelter, and manages its own water utility.

2.2 HAZARDS SUMMARY

2.2.1 CITY HAZARDS

A hazard is an event or condition that can cause fatalities, injuries, property and infrastructure damage, environmental harm, business disruptions, or other adverse impacts. Through the City's most recent hazard mitigation planning process (2021), the City evaluated natural, technological, and human-caused hazards that—regardless of likelihood—could affect City services and operations. The 2021 City of Redlands Local Hazard Mitigation Plan (LHMP) considered the 17 hazards listed in Table 2.2.1 City Hazards below.

Table 2.2.1 City Hazards

City Hazards	
Aircraft Accident/Incident	Infectious Disease
Civil Disturbance	Infestation
Dam Breach	Landslide
Drought	Technology Disruption
Earthquake	Terrorism
Energy Shortage/Power Outage	Train Accident/Incident
Extreme Temperature	Wildfire
Flood	Windstorm
Hazardous Material Accident	

Source: 2021 City of Redlands Local Hazard Mitigation Plan (LHMP)

2.2.2 COUNTY HAZARDS

San Bernardino County identified 18 hazards in its 2022 Multi-Jurisdictional Hazard Mitigation Plan (MJHMP), listed in Table 2.2.2 County Hazards on the next page. The hazards are ranked based on their probability of occurrence and potential impact.

Table 2.2.2 County Hazards

County Hazards	
Hazards	**Probability/Impact**
Climate Change	Medium Probability/Medium Impact
Dam Inundation	Low Probability/Medium Impact
Drought	High Probability/Medium Impact
Earthquake/Geologic Hazards	High Probability/High Impact
Extreme Heat	Medium Probability/Low Impact
Extreme Cold	Low Probability/Low Impact
Flood	High Probability/High Impact
Hazardous Waste	Probability/Impact Not Assessed
High Winds/Straight Line Winds	Low Probability/Low Impact
Hail	Medium Probability/Low Impact
Infestation	Medium Probability/Low Impact
Landslide	Medium Probability/Medium Impact
Lightning	Low Probability/Low Impact
Terrorism	Medium Probability/High Impact
Tornado	Low Probability/Low Impact
Volcanic Activity	Probability/Impact Not Assessed
Wildfire	High Probability/High Impact
Winter Storm/Heavy Snowfall	Low Probability/Low Impact

Source: 2022 San Bernardino County Multi-Jurisdictional Hazard Mitigation Plan (MJHMP)

2.2.3 COUNTY DISASTERS

San Bernardino County experienced 35 Federal Major Disaster Declarations between 1965 and 2020, including 13 fires, 18 severe weather events, one pandemic declared twice, and two earthquakes. During this same period, the County also received 20 Fire Management Assistance Declarations, beginning in 2003 (2025 SBCO EOP; 2022 SBCO MJHMP).

2.3 PLANNING ASSUMPTIONS

Planning assumptions establish the conditions the City accepts as factual for planning purposes, enabling effective execution of the EOP and facilitating decision-making when information is limited or uncertain. Planning assumptions include:

- Major emergencies and disasters will require a multi-agency, multi-jurisdictional response
- Major emergencies and disasters may require an extended commitment of personnel and other resources from involved agencies and jurisdictions
- Major emergencies and disasters may overburden local resources and necessitate mutual aid assistance
- Mutual aid assistance, critical equipment, essential supplies, and technical expertise may be limited or unavailable during regional or national disasters
- Major emergencies and disasters may pose serious long-term threats to public health, property, the environment, and the local economy
- Effective use of alert and warning systems reduces loss of life and property
- Vulnerable critical facilities have been identified and secured to protect life, personnel, equipment, and infrastructure
- The City maintains an EOC to manage all emergency management activities during major emergencies and disasters
- City departments develop and maintain internal operations plans and standard operating procedures that support this EOP
- The City conducts regular training and exercises to test the EOP and trains staff, using after-action reviews to drive continuous improvement
- Staff responsible for EOP implementation and disaster response have reviewed, exercised, and updated the Base Plan, Annexes, and SOPs, and are familiar with their roles
- Staff responsible for EOP implementation and disaster response have been trained in SEMS and NIMS and possess a full working knowledge of both systems
- City departments have integrated SEMS and NIMS into preparedness planning and apply both systems during disaster response operations

3. CONCEPT OF OPERATIONS

3.1 GENERAL OVERVIEW

The functions performed by City departments during emergency operations generally align with their normal functions. Tasks and operations that do not contribute directly to the emergency may be suspended or redirected during an emergency or disaster, and efforts that would typically be assigned to those tasks will be redirected toward emergency and disaster relief efforts.

If the emergency exceeds the City's capability to manage, assistance may be requested from San Bernardino County and the State. If the emergency exceeds the State's capability to manage, assistance may be requested from the Federal government.

This section of the plan outlines how the plan will be activated and implemented, with the purpose of protecting lives, property, and the environment of the City.

3.2 PHASES OF EMERGENCY MANAGEMENT

Emergency management consists of interrelated phases or mission areas that encompass activities before, during, and after a disaster; however, not every disaster necessarily includes all indicated phases. The Mitigation, Prevention, and Protection phases are combined for the purposes of this section.

All City departments have responsibilities in all phases.

3.2.1 PREPAREDNESS

The Preparedness phase consists of activities carried out before an emergency or disaster to build operational capabilities and ensure effective response. Preparedness activities include:

- Mitigation activities
- Emergency/disaster planning
- Training and exercises
- Public education on preparedness

Disaster plans are reviewed to guide response operations and maximize available resources. Planning activities include conducting hazard analyses, training response personnel, and enhancing public information and communication systems. Critical

facilities implement final preparations, additional staff and resources are mobilized, and warning systems are used both for testing and to inform staff of ongoing efforts.

3.2.1.1 COMMUNITY PREPAREDNESS

Public awareness and education are foundational to building community resilience from the ground up, empowering individuals and neighborhoods to sustain themselves during emergencies until first responders are able to provide assistance.

The City offers the following resources to enhance community preparedness:

- Community Emergency Response Team (CERT) Training
- Emergency Alerts
- Emergency Services
- Redlands Emergency Communications Group

San Bernardino County offers the following resources to enhance community preparedness:

- Emergency Alerts
- Preparedness Resources
- Volunteer Programs
- Listos (Spanish Language Resources)

3.2.2 MITIGATION/PREVENTION/PROTECTION

Mitigation, prevention, and protection strategies reduce disaster risks and impacts. Mitigation minimizes long-term risks, prevention avoids disasters, and protection safeguards people, property, and infrastructure.

3.2.2.1 MITIGATION

Mitigation reduces long-term risks to life and property from hazards. Mitigation efforts include amending local ordinances and statutes, such as zoning ordinances, building codes, and other enforcement codes; initiating structural retrofitting measures; assessing tax levies or abatements; emphasizing public education and awareness; undertaking flood control projects; removing fuel in areas with a high potential for wildfires; and assessing and altering land use planning.

3.2.2.2 PREVENTION

Prevention involves proactive measures to avoid or reduce disasters, such as enforcing safety regulations, conducting hazard assessments, and promoting public awareness. This helps prevent disruptions and minimize impacts. By focusing on prevention, the City can better prepare for threats and reduce vulnerabilities to various hazards.

3.2.2.3 PROTECTION

Protection safeguards people, property, and critical infrastructure from threats and hazards. It includes security measures around facilities, comprehensive emergency response plans, and robust communication and monitoring systems. Securing critical infrastructure enhances preparedness and aims to maintain continuous uninterrupted essential services.

3.2.3 RESPONSE

The Response phase includes any action taken before, during, or after an emergency situation to save lives, minimize damage to property, and enhance the effectiveness and speed of recovery. The response phase can be divided into:

- Pre-emergency response
- Emergency response

3.2.3.1 PRE-EMERGENCY RESPONSE

When a disaster is inevitable, actions are precautionary and emphasize protection of life. Typical responses might be:

- Review NIMS and SEMS SOPs
- Develop procedures for mobilizing public safety personnel and repositioning resources and equipment
- Develop a process for managing incidents using the Incident Command System (ICS) in coordination with the Police Department and Fire Department
- Notify and brief the City Manager and senior staff as appropriate
- Evacuate threatened populations to safe areas
- Alert populations by Rave Alert, City website, social media, radio, television, etc. and advise them on safety measures to be implemented

- Identify and request mutual aid
- Coordinate with the City Manager's Office on the process and procedure for activating Citizen Emergency Response Team (CERT) members and recruiting volunteers and additional staff (including the procedure for registering them as Disaster Service Workers)
- Review maps of specific hazards (e.g., hazmat, flood inundation areas, earthquake faults) to be used by City departments and emergency responders
- Prepare to mobilize CERT-trained personnel, auxiliary, and volunteer staff
- Pre-position resources and equipment
- Request a local emergency proclamation

3.2.3.2 EMERGENCY RESPONSE

During this phase, emphasis is placed on saving lives and property, controlling the situation, and minimizing the impacts of the emergency or disaster. Immediate response is accomplished by the City through timely and effective deployment. One of the following conditions will apply during this phase:

- The incident can be managed by the City
- The City requires mutual aid
- The City can provide mutual aid either locally or through the San Bernardino County Operational Area (OA)

The City will give priority to the following operations:

- Dissemination of accurate and timely alerts and warnings to the public
- Situation analysis
- Resource prioritization, allocation, and control
- Evacuation and rescue operations
- Medical care operations
- Mass care (i.e., reception, feeding, and shelter operations)
- Access and perimeter control
- Public health operations

- Restoration of vital services and utilities
- Multi-agency coordination

When local resources are insufficient, the City will use established mutual aid agreements and, if needed, request mutual aid through the appropriate San Bernardino County Mutual Aid Coordinator or the San Bernardino County OA EOC. More information about mutual aid is provided in **Section 8: Mutual Aid and Resource Management** of this EOP.

Depending on the emergency's severity, the San Bernardino County OA EOC may activate to support operations. If a State of Emergency is declared, State agencies will assist as coordinated by Cal OES, which may activate the State Operations Center (SOC) in Sacramento. The Cal OES Southern Region in Los Alamitos will support the San Bernardino County OA EOC. If a Presidential Declaration is granted, a State Coordinating Officer (SCO) will be appointed to manage recovery efforts with Federal agencies.

3.2.4 RECOVERY

Recovery operations establish procedures for accessing government programs that provide individual and public assistance after a disaster. Recovery may extend well beyond the conclusion of an emergency to restore normalcy, secure disaster response funding, and incorporate lessons learned into future preparedness and mitigation efforts. Short-term recovery focuses on damage assessment and restoring critical life-support systems to minimum operating levels. Long-term recovery and community rebuilding efforts may continue for many years.

Figure 3.2.4 below represents the disaster recovery process.

Figure 3.2.4 Disaster Recovery Process

Source: FEMA National Disaster Recovery Framework, 2024

Recovery Operations are further detailed in **Section 3.17: Recovery Operations** of this EOP.

3.3 STANDARDIZED EMERGENCY MANAGEMENT SYSTEM

The City has fully adopted the California Standardized Emergency Management System (SEMS), which is required by the California Government Code § 8607(a) for managing multiagency and multijurisdictional responses to emergencies in California. In times of emergency or disaster, the City will coordinate with other cities, San Bernardino County, the State, and the Federal government.

SEMS unifies all elements of California's emergency management community into a single integrated system and standardizes key elements. SEMS incorporates the use of the Incident Command System (ICS), California Disaster and Civil Defense Master Mutual Aid Agreement, the OA concept, and multiagency coordination. State agencies are required to use SEMS, and local government entities must use SEMS to be eligible for any reimbursement of response-related costs under the State's disaster assistance programs.

Unified Command (UC) allows multiple agencies with responsibility for an incident to manage an incident by establishing a common set of incident objectives and strategies. This is accomplished without losing or abdicating agency authority, autonomy, responsibility, or accountability.

3.3.1 SEMS ORGANIZATIONAL LEVELS

SEMS consists of five organizational levels:

1. **Field Response Level:** Commands emergency response personnel and resources to carry out tactical decisions and activities in direct response to an incident or threat
2. **Local Government Level:** Manages and coordinates a jurisdiction's overall emergency response and recovery activities
3. **Operational Area (OA) Level:** Manages and coordinates information, resources, and priorities among local governments within the San Bernardino County OA and serves as the coordination and communications link between the local and regional levels
4. **Regional Level:** Manages and coordinates information and resources among OAs within a mutual aid or administrative region (designated pursuant to

California Government Code § 8600) and between the OAs and the State. The regional and State levels coordinate overall State support for emergency response and recovery activities

5. **State Level:** Manages State resources in response to the emergency needs of the other levels, manages and coordinates mutual aid among the mutual aid regions and between the regional and State levels, and serves as the coordination and communication link with the Federal disaster support system

3.3.2 SEMS ORGANIZATIONAL FUNCTIONS

SEMS organizes the EOC into five primary functions:

- **Management Function:** Responsible for overall emergency policy and coordination through joint efforts of governmental agencies and private organizations
- **Operations Function:** Responsible for coordinating jurisdictional operations to support the emergency by implementing the action plan
- **Planning & Intelligence Function:** Responsible for collecting, evaluating, and disseminating information; developing the action plan in coordination with other functions; and maintaining incident records and documentation
- **Logistics Function:** Responsible for providing facilities, services, personnel, equipment, and materials to support incident response
- **Finance & Administration Function:** Responsible for all incident financial activities and administrative aspects not assigned to the other functions

3.3.3 IMPLEMENTING SEMS

SEMS will be used when the City EOC is activated or when a Local Emergency, as defined in California Government Code § 8558(c), is proclaimed. When the EOC is activated, communications and coordination will be established between the Incident Commander (IC) and EOC.

Communications and coordination will be established between the City EOC and any local and State response agencies having jurisdiction on an incident occurring within City boundaries. As defined in California Government Code § 8607(a), the City will use multi-agency coordination to facilitate decisions for City-level emergency response activities.

3.4 NATIONAL INCIDENT MANAGEMENT SYSTEM

The City has fully adopted the National Incident Management System (NIMS), as established by Homeland Security Presidential Directive-5 (HSPD-5), which integrates best practices into a consistent, flexible, and adjustable nationwide approach for emergency management.

Using NIMS, Federal, State, local and tribal governments, as well as private sector and non-governmental organizations work together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. Federal and State government agencies are required to use NIMS, while local government agencies and special districts must use NIMS to be eligible for Federal funding for emergency and disaster preparedness activities.

3.5 INCIDENT COMMAND SYSTEM

The Incident Command System (ICS)—which is part of both SEMS and NIMS—is a standardized, on-scene, all-hazards incident management approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private
- Establishes common processes for planning and managing resources

ICS is used in all levels of government and many non-governmental organizations and the private sector. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. ICS is also applicable across disciplines.

ICS is structured to facilitate activities in five major functional areas:

- **Command:** Responsible for directing response activities, including developing strategies, managing resources, and planning overall operations
- **Operations:** Responsible for coordinating the incident's tactical response and resources and for accomplishing incident-specific objectives
- **Planning:** Responsible for ongoing situation assessment; collection, evaluation, dissemination, and use of incident or event information; and

managing incident intelligence, including the status of response efforts and incident resources, to assist in the development of contingency plans

- **Logistics:** Responsible for providing facilities, services, and materials, including transportation and fuel, shelter, personal hygiene, food, potable water, tools, medical attention and supplies, communications, and relief personnel
- **Finance & Administration:** Responsible for tracking incident costs and evaluating the financial considerations of the incident

3.6 EMERGENCY SUPPORT FUNCTIONS

The City utilizes SEMS as required by California Government Code § 8607(a), structuring emergency management into the five key functions.

San Bernardino County, the State of California, and the Federal government incorporate the Emergency Support Function (ESF) model for providing emergency support during EOC activations. ESFs are designed to bring together discipline-specific stakeholders at all levels of government to collaborate and function within the five phases of emergency management.

Although the City does not use the Emergency Support Function (ESF) model, **Appendix F: ESF Crosswalk** of this EOP provides a crosswalk of ESFs to support coordination with San Bernardino County, Cal OES, and FEMA.

3.7 EMERGENCY PROCLAMATIONS

3.7.1 LOCAL EMERGENCY

A Local Emergency may be proclaimed by City Council or the Director of Emergency Services (MC § 2.52.100). A Local Emergency proclamation by the Director of Emergency Services must be ratified by City Council within seven days. City Council must review the need to continue the proclamation at least every 60 days until it terminates the Local Emergency. The Local Emergency may be terminated by resolution when conditions warrant. Proclamations are normally made when there is an actual incident, threat of disaster, or extreme peril to the safety of people and property within the City caused by natural or man-made situations. The proclamation of a Local Emergency provides the City with legal authority to:

- Request that the Governor proclaim a State of Emergency

- Promulgate or suspend orders and regulations necessary to provide for the protection of life and property, including issuing orders or regulations imposing a curfew within designated boundaries
- Exercise full power to provide mutual aid to any affected area in accordance with local ordinances, resolutions, emergency plans, or agreements
- Request mutual aid support from the County and other jurisdictions
- Require the emergency services of any local official or employee
- Request necessary personnel and materials from any local department or agency
- Obtain vital supplies and equipment and, if required, immediately commandeer the same for public use
- Impose penalties for violation of lawful orders
- Conduct emergency operations without incurring legal liability for performance or failure of performance (see Article 17 of the Emergency Services Act for privileges/immunities)

3.7.2 STATE OF EMERGENCY

A State of Emergency may be proclaimed by the Governor when:

- Conditions of disaster or extreme peril exist which threaten the safety of persons and property within the State caused by natural or man-made incidents
- The Governor is requested to do so by local authorities
- The Governor finds that local authority is inadequate to cope with the emergency

When a State of Emergency has been proclaimed:

- The Governor shall, to the extent deemed necessary, have the right to exercise all police power vested in the State by the Constitution and the laws of the State within the designated area
- Jurisdictions may command the aid of citizens as deemed necessary to cope with an emergency

- The Governor may suspend the provisions of orders, rules or regulations of any State agency and any regulatory statute or statute prescribing the procedure for conducting State business
- The Governor may commandeer or make use of any private property or personnel (other than the media) in carrying out the responsibilities of their office
- The Governor may promulgate, issue, and enforce orders and regulations deemed necessary

3.7.3 STATE OF WAR EMERGENCY

Whenever the Governor proclaims a State of War Emergency, or if a State of War Emergency exists, all provisions associated with a State of Emergency apply, additionally:

- All State agencies and political subdivisions are required to comply with the lawful orders and regulations of the Governor which are made or given within the limits of his authority as provided for in the Emergency Services Act.

3.8 OPERATING CONDITIONS

Operating Conditions have been established to provide a general indicator of the level of seriousness of an incident, impending incident, and current or anticipated emergency conditions. Operating Conditions and related guidance for lead and support departments will guide the readiness and response actions necessary to handle actual or impending emergencies. Operating Conditions do not reflect EOC Activation Levels, which are described in **Section 3.10: EOC Activation Levels** of this EOP. Operating Conditions are provided in Table 3.8 below.

Table 3.8 – Operating Conditions

OPERATING CONDITIONS		
Level	**Description**	**Associated EOC Activation Level**
Green	Normal Operations	None
Yellow	Increased Readiness	Management Watch
Red	Emergency Operations	Level 3, 2, 1

3.8.1 NORMAL OPERATIONS

GREEN: Under Normal Operations, departments conduct planning, training, and exercise activities to fulfill their roles in the EOP. They are staffed and operate per normal business operations, while also preparing for the next operating condition.

This condition is not associated with any EOC Activation Level.

3.8.2 INCREASED READINESS

YELLOW: Under Increased Readiness, events or conditions pose an actual or potential threat to life and property in threatened areas. Departments are taking increased readiness activities before an impending or potential emergency. Department Operations Centers (DOCs) may be activated to facilitate information and resource management. Agencies, departments, and special districts should prepare for the next operating condition.

This condition may be associated with Management Watch.

3.8.3 EMERGENCY OPERATIONS

RED: During Emergency Operations, events significantly impact life and property in affected areas. The EOC is activated and staffed, with DOCs activated as needed. Departments are taking all appropriate response actions, including curtailing non-essential operations and implementing special staffing patterns. This status is maintained until conditions de-escalate. Agencies, departments, and special districts should prepare for sustained emergency operations.

This condition may be associated with EOC Activation Levels 3, 2 or 1.

3.8.4 NOTIFICATION AND MOBILIZATION OF RESPONSE FORCES

The following is the process for notifying and mobilizing response forces in the City of Redlands:

City of Redlands EOC Team:

- By the Emergency Management Specialist, Redlands Police Department Dispatch Center, or designated alternate. Notification will be made through the City's Rave alerting system (Rave) or email to text.

City of Redlands Police Department:

- By the Redlands Police Department Dispatch Center.

City of Redlands Fire Department:

- By the CONFIRE Communications Center or via the on-duty Battalion Chief.

City of Redlands Departments:

- By each Department Operations Center, on-call staff person, or department administrative center.

Mutual Aid:

- By the respective City department or Mutual Aid Coordinator. Mutual aid resources are managed consistent with Section 8: Mutual Aid and Resource Management of this plan.

3.9 EOC ACTIVATION AND DEACTIVATION

3.9.1 EOC ACTIVATION

The EOC will become activated:

- By order of the City Manager as the Director of Emergency Services designated under MC § 2.52.080, or the Assistant City Manager(s) as Assistant Director(s) of Emergency Services, or the Fire Chief as the Emergency Manager, or a designee, or
- Upon the proclamation of a local emergency or when conditions exist that may warrant such a proclamation, consistent with the authority granted in MC § 2.52.100, or
- When the Governor has proclaimed a State of Emergency in an area, including the City of Redlands, or
- At the proclamation of a State of War Emergency, as defined by the California Emergency Services Act, or
- Upon a Triggering Event identified within this section.

3.9.2 TRIGGERING EVENTS

The following events may trigger the activation of the EOC:

- Damaging earthquake, wildfire, flood, or other impactful event
- Severe weather warning
- Significant commitment or draw-down of City emergency resources

- Regularly scheduled emergency exercises or training activities
- City special or planned events of significance
- Any incident that inhibits the City's ability to deliver essential services
- Any situation that requires coordinated, multi-department action through the EOC to protect life, property, or public safety

3.9.3 EOC SETUP AND STAFFING

Notification will be made to the Fire Chief as the Emergency Manager (or designee), who will oversee and coordinate the EOC's physical activation, setup, and staffing. The Fire Chief as the Emergency Manager (or designee) is responsible for maintaining the readiness of the EOC.

3.9.4 EOC NOTIFICATION AND MOBILIZATION

Notification of an EOC activation will be initiated by the City Manager, Assistant City Manager, Fire Chief, or their designee**.** Upon direction to activate, the Emergency Management Specialist, Police Communications Center, or the Duty Fire Battalion Chief will carry out the notification using the City's RAVE Alerting System, supplemented as needed by telephone, text message, or email using established City contact lists and pre-identified EOC staffing rosters.

Notifications regarding impending or actual emergencies may originate from the Redlands Police Department Communications Unit, Redlands Fire Department, CONFIRE Communications Center, San Bernardino County Sheriff's Department, San Bernardino County Office of Emergency Services (OES), National Weather Service, or a utility provider.

3.9.5 NOTIFICATION TO THE OPERATIONAL AREA

The San Bernardino County OES will be notified of a City EOC activation as soon as practical. The responsibility for making this notification lies with the Director of Emergency Services/EOC Director, the EOC Manager/Coordinator, or a designee. The County will subsequently be notified when the EOC is deactivated.

3.9.6 ACTIVATION OF THE ALTERNATE EOC

The Alternate City EOC will be activated whenever the Primary City EOC is uninhabitable, inaccessible, or located in a high-hazard zone due to an emergency.

3.9.7 EOC DEACTIVATION

The Director of Emergency Services/EOC Director or Assistant Director(s) of Emergency Services will direct the deactivation of the EOC when conditions no longer require its operation. As the situation deescalates, the EOC will be deactivated, and all positions and functions will be demobilized.

3.10 EOC ACTIVATION LEVELS

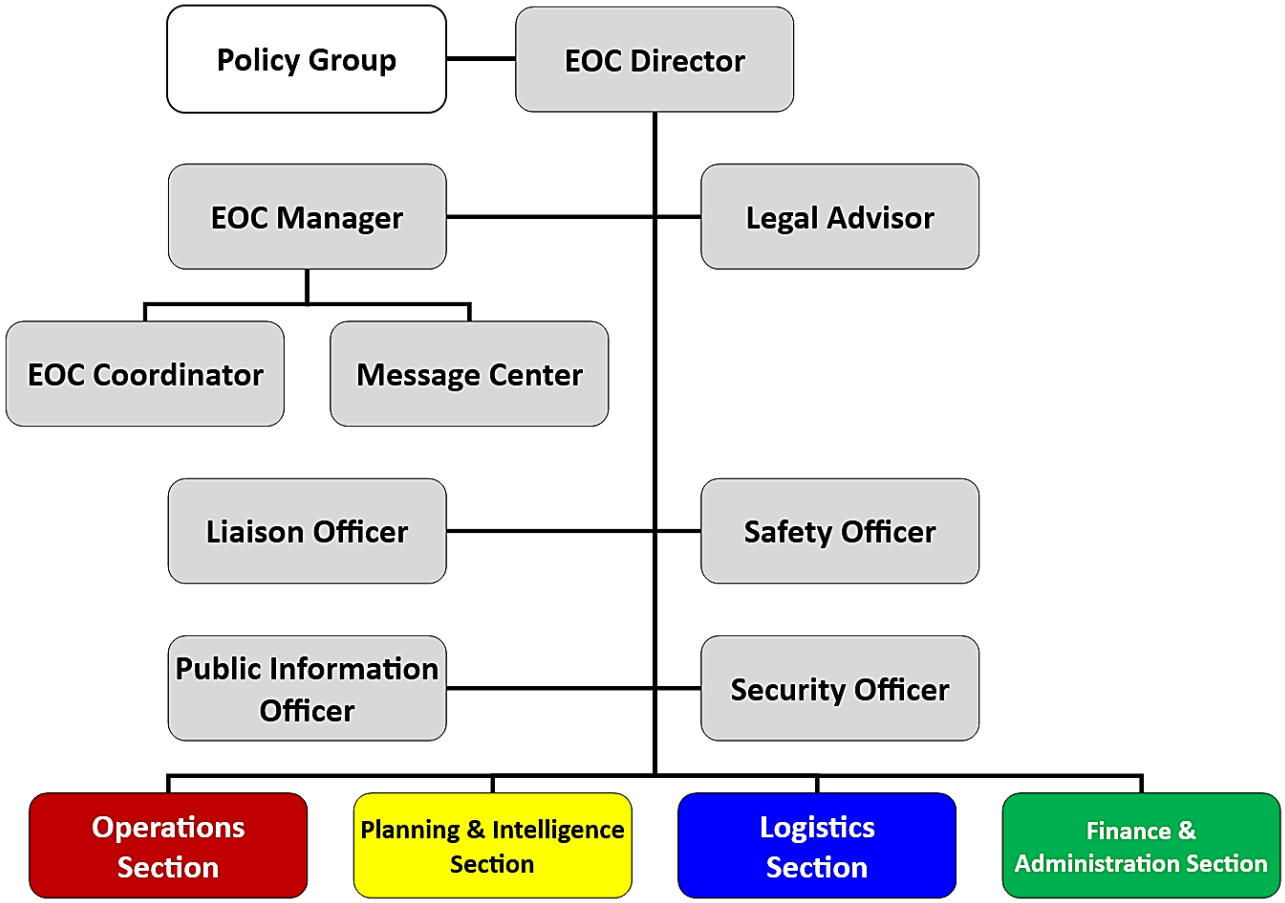
EOC activation levels are used to describe the scale and severity of an incident, the extent of coordination required, and the degree of support required from City departments and other agencies.

3.10.1 LEVEL 3: MINIMAL STAFFING

Impending or actual emergencies have prompted an increase in activity at the EOC. Essential EOC functions are activated, commensurate to the impending or actual emergency.

Level 3 staffing may include the Management Section, Section Chiefs, and any required support personnel. Other EOC Team members may be required to be readily available by phone. Level 3 staffing is illustrated in Graphic 3.10.1 on the next page.

Graphic 3.10.1 – Level 3 Staffing

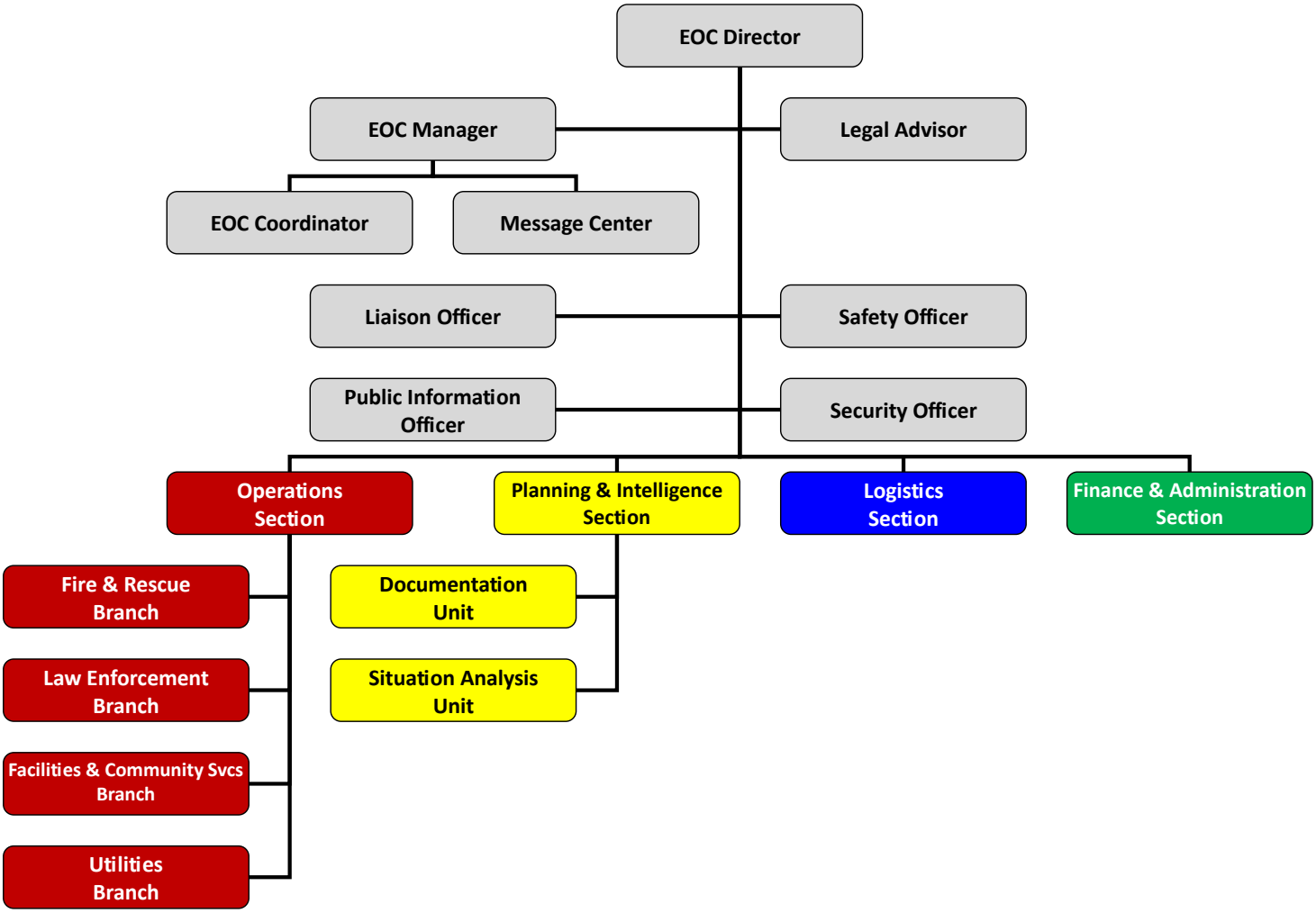


3.10.2 LEVEL 2: PARTIAL STAFFING

Impending or actual emergencies have prompted an increase in activity at the EOC. Essential EOC functions are activated, commensurate to the impending or actual emergency.

Level 2 staffing may include the Management Section, Section Chiefs, Branch Directors, and any required support personnel. Other EOC Team members may be required to be readily available by phone. Level 2 staffing is illustrated in Graphic 3.10.2 below.

Graphic 3.10.2 – Level 2 Staffing

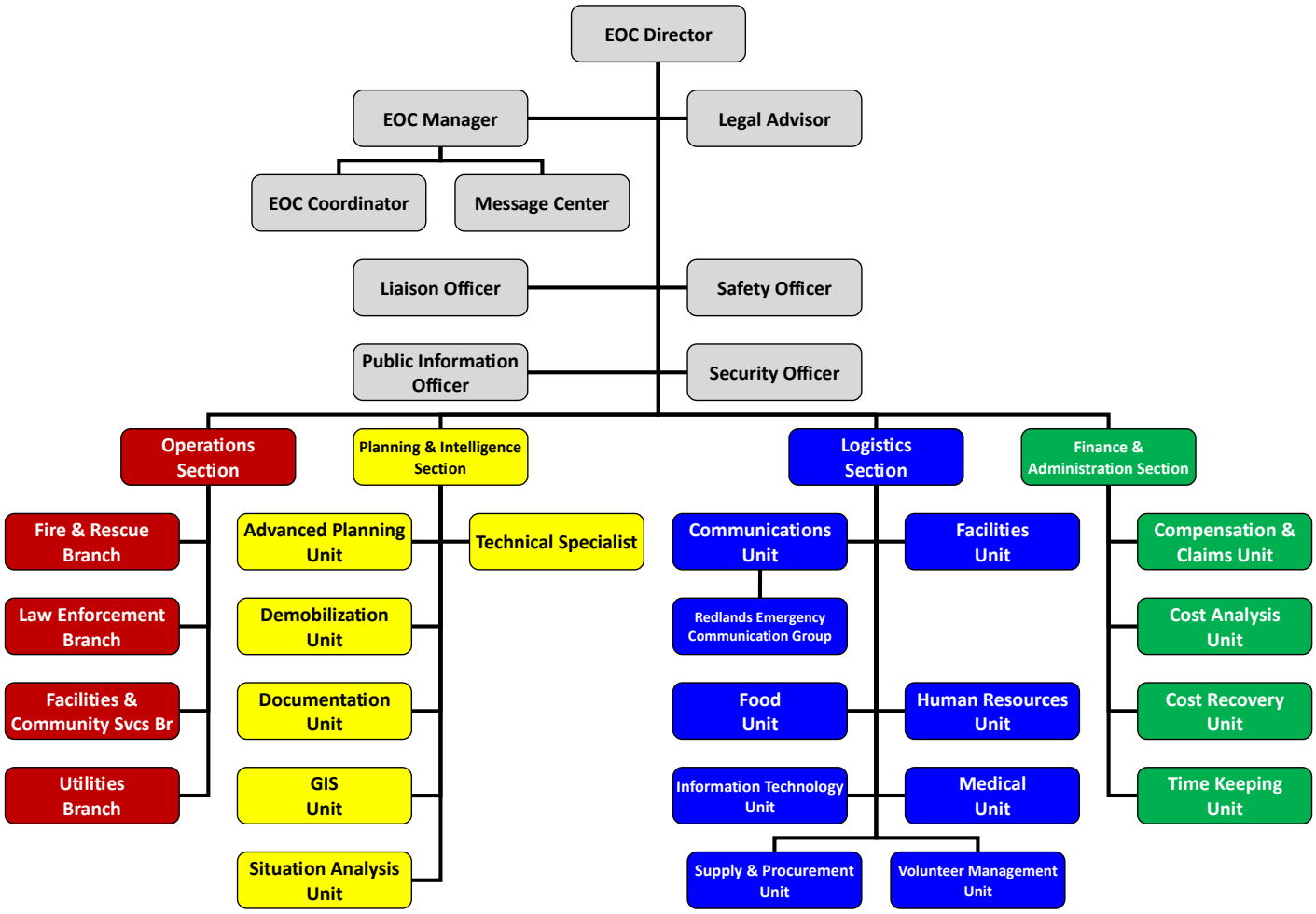


3.10.3 LEVEL 1: FULL STAFFING

Actual emergencies have prompted the full and complete activation of the City EOC. Essential EOC functions are activated commensurate to the emergency.

Level 1 staffing may include the Management Section, Section Chiefs, Branch Directors, Unit Leaders, and all required support personnel. Level 1 staffing will generally include all EOC functions and positions. Other EOC Team members may be required to be readily available by phone. Level 1 staffing is illustrated in Graphic 3.10.3 below.

Graphic 3.10.3 – Level 1 Staffing



3.10.4 MANAGEMENT WATCH

City departments or management staff may be required to monitor an evolving or potential emergency incident without activation of the EOC. This is referred to as a

Management Watch and involves close situational monitoring conducted outside of the EOC. A Management Watch does not constitute an EOC activation level.

3.11 EOC STAFFING MATRIX FOR CITY DEPARTMENTS

Each EOC function is assigned to one or more City departments. Department EOC assignments are found in **Appendix E: EOC Staffing Matrix for Departments** of this EOP.

3.12 EOC ACTION PLANS

At local, OA, regional and State levels, the use of EOC Action Plans provide designated personnel with knowledge of the objectives to be achieved and the steps required for achievement. EOC Action Plans not only provide direction, but they also serve to provide a basis for measuring achievement of objectives and overall system performance.

EOC action planning is an important management tool that involves:

- A process for identifying priorities and objectives for response or recovery efforts
- Documentation of the priorities, objectives, tasks, and personnel assignments

The action planning process should involve Management and General Staff along with other EOC elements, special district representatives, and other agency representatives as appropriate. The Planning & Intelligence Section is normally responsible for the development of the EOC Action Plan and the facilitation of action planning meetings.

EOC Action Plans are developed for a specified operational period that may range from a few hours to 24 hours. The operational period is determined by first establishing a set of priority actions that need to be performed. A reasonable time frame is then established for accomplishing those actions. EOC Action Plans need not be complex but should be sufficiently detailed to guide EOC elements in implementing the priority actions.

An EOC Action Plan is strategic and therefore not meant to replace a field-based Incident Action Plan (IAP). The EOC Action Plan should be coordinated with any existing IAPs.

3.13 CULTURAL COMPETENCE

Cultural competence is the ability to understand, respect, and appropriately respond to the diverse values, beliefs, and customs of different cultural groups. It is a critical component of equitable emergency preparedness, response, and recovery since disasters may disproportionately impact culturally diverse communities.

This EOP incorporates the requirements of California Government Code § 8593.3.5, which mandates consideration of cultural competence in all phases of emergency management. Key considerations include:

- Culturally and linguistically appropriate emergency communications, including the use of interpreters and translators
- Inclusive planning for evacuation and sheltering operations
- Culturally informed mitigation and prevention efforts
- Planning processes that engage qualified representatives from diverse community groups
- Preparedness education using culturally relevant outreach strategies and materials

The Director of Emergency Services/EOC Director will oversee implementation of these activities, with coordination handled by the appropriate EOC Sections and Branches.

3.14 DISABILITIES OR ACCESS AND FUNCTIONAL NEEDS POPULATIONS

Populations with disabilities or access and functional needs (DAFN) are community members who may require additional support before, during, and after an emergency in areas such as maintaining independence, communication, transportation, supervision, language, and medical care.

The City has identified its DAFN populations using the most recent US Census Bureau statistics:

- 15% of the population is 65 years and over
- 7.7% of the population is under 65 years and disabled
- 28.4% of the population speaks a language other than English at home

The EOP includes provisions to ensure that emergency notification, evacuation, transportation, and sheltering operations accommodate DAFN individuals. The City's planning efforts include:

- Notification and warning procedures, including Reverse 911
- TDD/TTY contact and captioned cable alerts for the hearing-impaired
- Accessibility of emergency information in multiple formats
- Language interpretation through staff skills and service contracts
- ADA-compliant access to facilities and shelters
- Transportation assistance for those requiring physical support
- Evacuation planning and emergency transportation coordination
- Accessibility for mobility devices, service animals, and medical needs (e.g., medications, refrigeration, backup power)

3.14.1 REQUIREMENTS OF THE AMERICANS WITH DISABILITIES ACT

Access to emergency services shall not be denied on the basis of race, color, national origin, sex, age, or disability. The City will ensure that all phases of emergency management address the needs of individuals protected under the Americans with Disabilities Act (ADA).

Pursuant to ADA Title II Regulations, State and local governments must ensure that programs, services, and activities are accessible to people with disabilities. This obligation extends to:

- Physical accessibility of facilities, programs, services, and events
- Policy modifications necessary to provide equal opportunity for participation
- Effective communication to ensure individuals with DAFN can receive, understand, and act upon information during all phases of an incident

3.15 ANIMAL CARE CONSIDERATIONS

During EOC activations, animal care needs will be addressed by the Animal Services Division within the City's Facilities & Community Services Department.

3.15.1 PETS ACT

The Pets Evacuation and Transportation Standards Act of 2006 (PETS Act) directs that State and local emergency preparedness plans address the needs of people with pets and service animals after a major disaster, including the rescue, care, and sheltering of animals. The PETS Act amends the Stafford Act, and requires evacuation plans to consider the needs of individuals with household pets and service animals, prior to, during, and after a major disaster or emergency.

3.15.2 CALIFORNIA ASSEMBLY BILL 781

California Assembly Bill 781, which created California Government Code § 8593.10, mandates that cities update their emergency plans to designate at least one emergency shelter capable of accommodating individuals with pets upon the next revision of their plans.

The City maintains one emergency shelter that is compliant with California Assembly Bill 781 and has a Memorandum of Understanding (MOU) with a facility capable of sheltering larger animals. These shelters are identified in **Annex 3: Response Plan (2022)** of this EOP.

3.16 RECOVERY ORGANIZATION

City recovery operations will be managed by the Director of Emergency Services/EOC Director until a Recovery Manager is appointed, who will report to the Director unless otherwise designated.

Until a dedicated Recovery Organization is established, the EOC or its components will fulfill recovery functions. Coordination may involve City departments, community-based organizations, businesses, utilities, non-governmental organizations (NGOs), San Bernardino County departments, OA partners, the Joint Field Office (JFO), and FEMA.

3.17 RECOVERY OPERATIONS

The recovery phase of an emergency or disaster is often defined as restoring a community to its pre-disaster conditions. In other words, recovery refers to the actions taken by the City following a disaster to restore normalcy. Effective recovery consists of an array of interdependent and coordinated actions. The specific approach to recovery operations following a disaster will be determined by the location, type, magnitude, and effects of the incident. Recovery operations are

divided into three phases: short-term, mid-term, and long-term. All phases will be coordinated by the City EOC.

The City maintains a separate **Disaster Recovery Plan (2024)**.

3.17.1 SHORT-TERM RECOVERY

Short-term recovery refers to the measures taken by the City following a disaster. It addresses the health and safety needs beyond rescue, the assessment of the scope of damages and needs, the restoration of basic infrastructure, and the mobilization of the National Disaster Recovery Framework organizations and resources. This includes restarting and/or restoring essential services for recovery decision-making. Effective recovery consists of a complex array of interdependent and coordinated actions.

The goal of short-term recovery is to restore City services to at least minimal capacity operations. Short-term recovery includes:

- Assessment of the extent and severity of damages to homes and other property
- Restoration of services generally available in communities, such as water, food, and medical assistance
- Professional counseling when the sudden changes resulting from the emergency have resulted in mental anguish and inability to cope
- Utility and infrastructure restoration
- Expanded social, medical, and behavioral health services
- Re-establishment of City government operations
- Transportation route restoration
- Debris removal and clean-up operations
- Abatement and demolition of hazardous structures

3.17.2 MID-TERM RECOVERY

Mid-term recovery efforts will prioritize the restoration of community lifelines and essential services, reestablishing access to food and fuel, and transitioning mass care operations into other forms of assistance. Mid-term recovery includes:

- Survivor care including housing, medical, emotional, behavioral, legal, and financial support
- Survivor reunification to reunite displaced persons with family networks
- Restoring community lifelines, including safety and security; food, water, and shelter; health and medical; energy (power and fuel); communication, transportation, and hazardous materials
- Debris management on public and private property
- Damage and safety inspection of homes, businesses, schools, and infrastructure

3.17.3 LONG-TERM RECOVERY

Long-term recovery consists of actions that will return City functions back to normal pre-disaster levels of service. It is critical that the documentation functions during response continue and expand into long-term recovery. The major objectives of long-term recovery operations include:

- Coordination of delivery of long-term social and health services
- Re-establishment of the local economy to pre-disaster levels
- Recovery of disaster response costs
- Integration of hazard mitigation strategies into recovery planning and operations

Failure to strictly account for damage documentation and personnel costs can result in loss of reimbursement.

3.17.4 FINANCIAL COST RECOVERY

In the months and years following a disaster, cost recovery will be focused on making individuals, businesses, and governments "whole" again. Financial cost recovery activities may include:

- Connecting survivors with Individual Assistance (IA) programs
- Connecting businesses and industries with financial assistance, including disaster loans from the Small Business Administration
- Restoring government entities through Public Assistance (PA) programs and Fire Management Assistance Grants for wildfire recovery

3.17.5 DAMAGE ASSESSMENT

In the initial hours following a disaster, it is critical that the City conduct a Rapid Needs Assessment (RNA), which collects data to estimate the extent of the damage. The EOC Planning & Intelligence Section, in coordination with the Operations Section and Finance & Administration Section, will organize damage reporting. The Finance & Administration Section will calculate cost and cost-recovery reporting. The City will submit its damage reports to the San Bernardino County OA, likely through an online portal or via email.

Within several days of the disaster, the City will coordinate with San Bernardino County and the State to conduct an Initial Damage Assessment (IDA), which captures damage information and impacts that may influence eligibility for State or Federal support or assistance. Following the IDA, the State will verify the data to ensure the level of damage caused by the disaster rises to the level of State or Federal support eligibility and meets the required indicators.

If the IDA indicates that the disaster is eligible for Federal support, then the State will request a Joint Preliminary Damage Assessment (JPDA) from the Federal government. Once the FEMA Regional Office reviews the State request for a JPDA and validates the IDA information, the JPDA Team—consisting of local and State governments in coordination with FEMA and the Small Business Administration (SBA)—will conduct site visits and assess damages, compile cost estimates and documentation, and assess damage assessment information to support a major disaster declaration request.

3.17.6 DISASTER ASSISTANCE

Federal disaster assistance is divided into two forms: Individual and Public Assistance. Individual Assistance is provided by FEMA to individuals and families who have sustained losses due to disasters. Public Assistance can fund the repair, restoration, reconstruction, and replacement of a public facility or infrastructure damaged or destroyed by a disaster. The Federal government also offers non-Stafford Act disaster relief programs.

State disaster assistance may be available through the California Disaster Assistance Act (CDAA).

Recovery plans should address all types of assistance, methods of acquiring help, restrictions, and other pertinent information.

3.17.6.1 INDIVIDUAL ASSISTANCE

Individual Assistance (IA) consists of the following services provided to individuals and families:

- **Disaster Housing Assistance Program:** Provides temporary housing to disaster victims during presidentially declared disasters. This Federal program is administered by FEMA.
- **Disaster Mortgage and Rental Assistance Program:** Provides grants for home-related mortgage or rent payments to disaster victims, who because of a disaster have lost their job or business and face foreclosure or eviction from their homes. This Federal program is available under a presidentially declared disaster.
- **Housing and Urban Development (HUD) Program:** Offered to families that meet certain income guidelines and may provide a percentage of the rental cost for a limited period to disaster victims. This program is available under a presidentially declared disaster.
- **Small Business Administration (SBA):** Provides low interest loans to businesses and individuals who have suffered disaster losses. This program is automatically implemented following a presidential disaster declaration for Individual Assistance or may be implemented at the request of the Governor.
- **Individual and Family Grant Program (IFGP):** Provides grants to disaster victims who are not eligible for SBA loans. This program is available under a presidentially declared disaster.
- **Cora Brown Fund:** Provides disaster victims with assistance, provided they are not eligible for any other disaster assistance award from the government or other organizations. This program is available under a presidentially declared disaster.

3.17.6.2 PUBLIC ASSISTANCE

Public Assistance (PA) consists of various programs of disaster relief to the public and private nonprofit sectors:

- Debris Management
- Private Nonprofit Program (PNP)

- Safety Assessment Program (SAP)
- Technical Assistance Programs (TAP)
- Laws and Regulations

The public sector includes State and local government (City, County, special district). Private nonprofit includes certain eligible Private Nonprofits (PNP) or an Intermediary PNP applicant to receive State assistance for extraordinary costs incurred while aiding at the request of local agencies during a State disaster event.

FEMA processes PA grant funding according to the type of work the applicant undertakes. Eligible work is classified into Emergency Work and Permanent Work.

Emergency Work

- **Category A: Debris Clearance** – Clearance of debris, wreckage, demolition, and removal of buildings damaged beyond repair
- **Category B: Protective Measures** – Measures to eliminate or lessen immediate threats to life, public health, and safety

Permanent Work

- **Category C: Roads & Bridges** – All non-emergency work and any that may require more time for decision-making, preparation of detailed design, construction plans, cost estimates, and schedules
- **Category D: Water Control Facilities** – Includes flood control, drainage, levees, dams, dikes, irrigation works, and bulkheads
- **Category E: Public Buildings and Equipment** – Buildings, vehicles or other equipment, transportation systems, fire stations, supplies or inventory, higher education facilities, libraries, and schools
- **Category F: Utilities** – Water supply systems, sanitary sewage treatment plants, storm drainage, and light/power
- **Category G: Other** – Park facilities, public and private facilities, recreational facilities, and playground equipment

Federal funding guidelines for each of these categories are listed in the FEMA PA Program and Policy Guide, which can be found on the Cal OES website at https://www.caloes.ca.gov/wp-content/uploads/Recovery/Documents/FEMA-Public-Assistance-Policy-Guide-V4.pdf.

3.17.6.3 NON-STAFFORD ACT PROGRAMS

The Federal government provides recovery assistance through authorities and programs outside the Stafford Act. These programs may be implemented alongside Stafford Act programs under a disaster declaration. Depending on the program, the agencies assist recipients directly or through another State agency besides Cal OES. Examples include:

- **Federal Highway Administration (FHWA):** Under the Emergency Relief Program, the FHWA provides assistance to the Department of Transportation (Caltrans) and local governments for damage to roads, bridges, and other facilities on the Federal aid system. Caltrans implements this program on behalf of FHWA.
- **Natural Resources Conservation Service (NRCS):** Under the Emergency Watershed Protection Program, the NRCS provides assistance to State agencies and local governments for emergency work necessary to protect life, property, and public health and safety in watersheds damaged by a disaster, such as wildfire or flood.
- **U.S. Army Corps of Engineers (USACE):** Under the Rehabilitation and Inspection Program, the USACE assists in flood fighting, emergency repairs, and repairs to damaged facilities. The USACE provides this assistance for levees and other flood control works that meet pre-disaster program participation criteria.
- **U.S. Department of Housing and Urban Development (HUD):** HUD Community Development Block Grants may be requested by State and local governments for a wide range of recovery purposes.
- **Congressional Appropriations:** Congress may make disaster-specific appropriations that allow Federal agencies to provide assistance beyond existing authorities and programs. State coordination of this assistance depends on the nature of the appropriation and the Federal agency charged with its implementation.

3.17.6.4 CALIFORNIA DISASTER ASSISTANCE ACT

The California Disaster Assistance Act (CDAA) provides State financial assistance for recovery efforts to cities, counties, special districts, and certain eligible private nonprofit agencies after a Cal OES Director's Concurrence or the Governor's

Proclamation. CDAA may be implemented as a "standalone" funding source following a State disaster.

CDAA is available to cities, counties, and special districts to repair disaster-related damage to public buildings, levees, flood control works, channels, irrigation works, City streets, County roads, bridges, and other public works except those facilities used solely for recreational purposes. This program offers a percentage of the eligible cost to repair, restore, reconstruct or replace public property or facilities; to cover direct and indirect costs of grant administration with the Cal OES Director's concurrence; and to cover the cost of overtime and supplies used for response. The conditions for implementation of the CDAA are as follows:

- The Cal OES Director must concur with a local emergency declaration for permanent restoration assistance
- The Governor must proclaim a State of Emergency for disaster response and permanent restoration assistance
- The President must declare a major disaster or emergency for matching fund assistance for cost sharing required under Federal public assistance programs

Note: Local proclamations of emergency should, when known at the time of issuance, specify any requests being made to the State, including anticipated needs for California Disaster Assistance Act (CDAA) assistance.

3.17.7 NON-GOVERNMENTAL ORGANIZATIONS AND COMMUNITY BASED ORGANIZATIONS

Non-Governmental Organizations (NGOs) and Community-Based Organizations (CBOs), such as the American Red Cross and the Salvation Army, typically provide support to individuals and households who are displaced by a disaster and work with governmental organizations to support the transition from care and shelter operations to interim housing arrangements. Community organizations active before a disaster may expand their services to meet increased needs. Such groups include faith-based organizations, neighborhood health clinics, and food distribution agencies. NGOs and CBOs may provide a range of services such as donations management, emergency food, clothing and shelter, behavioral and spiritual counseling, assist with non-hazardous debris removal from private

property, as well as support of housing reconstruction. They provide these services independently or in coordination with Federal, State, and local efforts.

3.17.8 RECOVERY REPORTING AND DOCUMENTATION

Recovery reporting and documentation is the key to recovering eligible emergency response and recovery costs. Damage assessment documentation will be critical in establishing the basis for eligibility of disaster assistance programs. Without proper documentation, the County and local jurisdictions may be liable to FEMA for disaster recovery funding.

3.17.8.1 RECOVERY DOCUMENTATION

Recovery documentation information should include the location and extent of damage, and estimates of costs for debris removal, emergency work, and repairing or replacing damaged facilities to a non-vulnerable and mitigated condition. The cost of compliance with building codes for new construction, repair, and restoration will also be documented. The cost of improving facilities may be provided under Federal hazard mitigation grant programs. Documentation is the key to recovering expenditures related to emergency response and recovery operations. Documentation must begin at the field response level and continue as the disaster unfolds. The EOC Planning & Intelligence Section, in coordination with the Operations Section and Finance & Administration Section, organizes damage reporting.

3.17.8.2 AFTER-ACTION REPORTING

The California Code of Regulations § 2450(a) requires the submission of After-Action Reports to Cal OES within 90 days of the close of an incident period for locally declared emergencies for which the Governor proclaims a State of Emergency.

An After-Action Report serves the following important functions:

- Provides a source for documenting response and early recovery activities
- Identifies problems and successes during emergency operations
- Analyzes the effectiveness of the different components of SEMS
- Identifies, documents, and facilitates corrective action for implementing and tracking improvements to existing emergency response and recovery efforts

The Fire Chief as the Emergency Manager (or designee) is responsible for coordinating the After-Action Review process and ensuring the After-Action Report is submitted.

3.17.9 JOINT FIELD OFFICE

Following a Presidential Declaration of a Major Disaster or Emergency, a Joint Field Office (JFO) will be established in proximity to the disaster area. The JFO is the direction and coordination point for Federal assistance. The State will appoint a State Coordinating Officer (SCO) to serve as the State point of contact. A Federal Coordinating Officer (FCO) is appointed upon a Presidential Declaration of an Emergency or Major Disaster.

3.17.10 COMMUNITY LIFELINES

FEMA defines Community Lifelines as those services or systems that "enable the continuous operation of critical government and business functions and is essential to human health and safety or economic security."

Stabilizing lifeline services is the top priority in disaster response due to immediate threats to life and property. Community Lifeline descriptions help responders assess conditions and determine necessary recovery actions. The City EOC prioritizes lifeline restoration in its EOC Action Plan. Since many lifelines are managed externally, close coordination with utility providers and external organizations will be essential.

Graphic 3.17.10 – Community Lifelines

Source: FEMA

3.18 EMERGENCY FACILITIES

Emergency facilities supporting emergency operations are identified and described below.

3.18.1 PUBLIC SAFETY COMMUNICATIONS CENTERS

City calls for police, fire, and emergency medical services are dispatched from the following locations:

- Redlands Police Department Communications Unit

  1270 W. Park Ave, Redlands, CA 92373

- CONFIRE Communications Center

  1743 Miro Way, Rialto, CA 92376

3.18.2 DEPARTMENT OPERATIONS CENTERS

A Department Operations Center (DOC) is a coordination hub for specific disciplines—such as fire, police, public works, or utilities—to manage field-level emergency responses and support the EOC.

The City maintains the following DOCs:

- Police Department – Watch Commander's Office
- Fire Department – Duty Battalion Chief's Office
- Municipal Utilities & Engineering Department

3.18.3 PRIMARY/ALTERNATE EMERGENCY OPERATIONS CENTERS

The EOC is the location where centralized emergency management during large-scale emergencies and disasters takes place. The primary and alternate EOCs are provided in Table 3.18.3 below.

Table 3.18.3 – City Emergency Operations Centers

City Emergency Operations Centers	
Primary EOC	**Redlands Police Department** 1270 W. Park Ave, Redlands, CA 92373
Alternate EOC	**Redlands Wastewater Treatment Facility** 1950 Nevada St, Redlands, CA 92373

During EOC activations, the EOC Policy Group will meet at a location separate from the primary and alternate EOCs.

3.18.4 JOINT INFORMATION CENTER

The Joint Information Center (JIC) is a location where staff from various organizations with public information responsibilities can co-locate to perform critical emergency public information, crisis communications, and public affairs functions. The JIC for the City would be co-located with the EOC if needed.

3.18.5 INCIDENT COMMAND POST

The Incident Command Post (ICP) is the field location for primary tactical-level, on-scene incident command and management. It typically includes the Incident Commander (IC) and Command Staff, as well as other incident management officials, responders, public agency representatives, private-sector representatives, and non-governmental organizations.

3.18.6 STAGING AREA

A staging area is a temporary holding location for assigned resources, established by the Incident Commander or Operations Section Chief. It allows for the positioning and accounting of resources not immediately needed for an operational task. These areas are used to temporarily position personnel, supplies, and equipment while awaiting an assignment.

3.18.7 MOBILIZATION CENTER

A mobilization center is an off-incident location where emergency personnel and equipment are temporarily positioned while awaiting assignment, release, or reassignment. Unlike a staging area, it is generally activated and managed by the EOC. Mobilization centers support significant emergencies and disasters, serving as hubs for mutual aid resources.

3.18.8 EVACUATION RECEPTION CENTER

An evacuation reception center temporarily accommodates people displaced from their home, school, or business. It provides a safe and comfortable space for disaster survivors to receive relief until the incident concludes, or they transition to a mass care center or shelter. These centers are established for short-duration incidents where overnight assistance or a shelter is unnecessary, or as a temporary solution while a fully operational shelter is being set up, which can take several hours.

3.18.9 SHELTER

A shelter provides temporary care for those displaced by emergencies, offering sleeping accommodation and minimal necessities. Unlike evacuation reception centers, shelters are equipped for overnight stays and may operate alongside evacuation reception centers. Evacuees are encouraged to bring essentials like blankets, toiletries, and snacks. Shelters require significant planning, logistics, staffing, medical and mental health support, and security.

The City has designated 19 facilities to potentially serve as emergency shelter sites for displaced persons, along with two separate facilities for emergency animal sheltering. These shelters are identified in **Annex 3: Response Plan (2022)** of this EOP.

4. ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

All City departments and employees have a role during emergency response and recovery operations. City employees are also Disaster Service Workers, per California Government Code § 3100, and may be called into service during proclaimed or declared disasters.

The City's emergency operations and organizational structure are organized according to the concepts and principles of SEMS and NIMS.

4.1 CITY LEVEL

The City of Redlands Emergency Organization (MC § 2.52.140) consists of "all officers and employees of the City, together with those volunteer forces enrolled to aid them during an emergency, and all groups, organizations, and persons who may be in agreement or operation of law, including persons impressed into service," who are "charged with duties incident to the protection of life and property in the City during such emergency."

4.1.1 DIRECTOR OF EMERGENCY SERVICES

The City Manager is the Director of Emergency Services, having jurisdiction and full authority over the City's response and recovery to extraordinary emergencies and disasters. The Assistant City Manager or Assistant City Managers serve as Assistant Directors of Emergency Services. Alternates may be designated by the Director of Emergency Services.

4.1.2 CITY COUNCIL

City Council may promulgate orders and regulations necessary to protect life and property, including orders and regulations to impose curfews and stop price fixing. Members of the City Council will serve as liaisons to constituents regarding the City's disaster response and recovery efforts. They will also liaise with County, State, and Federal elected officials, as appropriate and necessary.

4.1.3 ELECTED OFFICIALS

Elected officials, including City Council members, play a non-operational support role during disasters. During an active disaster response, elected officials best serve the public by supporting—rather than directing—trained emergency personnel and EOC staff. Their role is non-operational, focused on maintaining public confidence

and enabling responders to stabilize the situation without interference. Strategic decisions by elected officials may follow once the incident is under control. The immediate priority remains rapid, coordinated action by emergency professionals.

4.1.4 DISASTER COUNCIL

The City of Redlands maintains a Disaster Council accredited by the State of California.

The City of Redlands Disaster Council Membership (MC § 2.52.050) consists of the Mayor (Chairperson); the City Manager/Director of Emergency Services (Vice-Chairperson); the Emergency Services Chief; "groups that support a strong team merging sectors of the community including elected officials, emergency management, first responders, volunteer services, major industry and commercial, healthcare and education"; and a Citizen Corps Council that "shall be created as a subgroup of the Disaster Council."

The City of Redlands Disaster Council powers and duties (MC § 2.52.060) state: "It shall be the duty of the City Disaster Council, and it is empowered, to develop and recommend for adoption by the City Council emergency and mutual aid plans and agreements."

The Disaster Council should meet at least once per year, upon call of the Chairperson, or upon call of the Vice-Chairperson (in the absence of the Chairperson).

4.1.5 EMERGENCY MANAGER

The Fire Chief, serving as the Emergency Manager, oversees the City's emergency management program, including preparedness, response, recovery, and mitigation activities. Responsibilities include maintaining the EOP, coordinating interagency training and exercises, and ensuring compliance with Federal and State emergency management standards. The position also manages public outreach, resource allocation, and continuity planning for critical City functions. The Emergency Manager serves as the primary liaison during disasters, facilitating communication between City departments, regional partners, and emergency services.

4.1.6 FIRST RESPONSE DEPARTMENTS

First response departments are operational entities tasked with responding to and recovering from emergencies and disasters.

In the City, first response departments include:

- Fire Department
- Police Department
- Facilities & Community Services Department

First response departments are responsible for developing policies, procedures, guidance, and resources to enable them to execute their responsibilities in the EOP.

4.1.7 DEPARTMENT OPERATIONS CENTER

A DOC is a coordination hub for specific disciplines—such as fire, police, public works, or utilities—to manage field-level emergency responses and support the EOC.

The City maintains the following DOCs:

- Police Department
- Fire Department
- Municipal Utilities & Engineering Department

4.1.8 EMERGENCY OPERATIONS CENTER

The EOC is a centralized location for coordinating emergency response activities. The City maintains primary and alternate EOCs, the locations of which are identified in **Section 3.18: Emergency Facilities** of this EOP.

4.1.9 EOC TEAM

The EOC Team is responsible for managing all aspects of EOC operations when activated. This team comprises City employees assigned to EOC functions, who provide strategic planning and direction from the EOC. Management Staff support the EOC Director, while General Staff handle SEMS functional aspects, and are led by Section Chiefs who report to the EOC Director.

4.1.10 EOC POLICY GROUP

The EOC Policy Group provides executive-level advice and subject-matter input to the Director of Emergency Services during an extraordinary emergency or disaster. The group helps shape interim policy considerations, identifies organizational impacts, and ensures that emergency regulations, proclamations, and orders are legally sound and operationally feasible. The Policy Group convenes as needed to

support the Director's decision-making and maintain alignment with City priorities and statutory requirements.

The Policy Group consists of the City Manager, Assistant City Manager(s), Mayor Pro Tem, Fire Chief, Police Chief, Finance Director, Human Resources Director, and the Facilities & Community Services Director. Together, these positions provide comprehensive executive coverage for legal authority, fiscal oversight, operational leadership, personnel and labor-relations considerations, and continuity of government.

The City Attorney (Legal Advisor) and City Clerk serve in a support role to the Policy Group, with the City Clerk responsible for documenting and recording all emergency orders and decisions made during Policy Group deliberations.

4.1.11 CITY DEPARTMENTS

City departments and divisions will ensure they can fulfill their emergency management responsibilities. They provide incident response and support, including staffing DOCs and the EOC Team using SEMS and NIMS principles. They conduct damage assessments, implement continuity and communication plans, establish programmatic operational strategies, and restore essential infrastructure and services.

4.1.12 DISASTER SERVICES WORKERS

According to California Government Code § 3101, a Disaster Service Worker (DSW) includes all public employees and all volunteers in any disaster council or emergency organization accredited by Cal OES. All City employees, full-time and part-time, are DSWs and may be called upon during emergencies and disasters. In an emergency, non-essential public employees may be released from their usual duties so that they can be reassigned to assist any agency or organization carrying out its emergency response duties. Employees acting as DSWs will be assigned duties within their scope of training, skill, and ability.

4.2 OPERATIONAL AREA LEVEL

California Government Code § 8559(b) defines an Operational Area (OA) as "an intermediate level of the State emergency services organization, consisting of a county and all political subdivisions within the county area." Political subdivisions include cities and special districts. An OA has an agreement in place that defines

roles and responsibilities, as well as jurisdictional authority in an emergency. The City is signatory to this agreement.

The San Bernardino County OES serves as the OA Coordinator for emergency management. OES is responsible for coordinating emergency response efforts across jurisdictions within the OA. It serves as the central hub for aligning information, resources, and priorities between local governments and regional authorities. OES facilitates multi-agency and inter-agency collaboration to support unified decision-making. Its role ensures cohesive, area-wide emergency management during incidents. When the emergency impacts OA jurisdictions, the designated OA Coordinator is responsible for ensuring direction, coordination and communication of policy decisions, resource needs, and priorities between OA jurisdictions and the State throughout the emergency (San Bernardino County EOP, 2025).

4.3 REGIONAL LEVEL

The regional level manages and coordinates information and resources among OAs. Cal OES has divided California into three administrative regions which are further divided into six mutual aid regions. The City is in the Southern Region and Mutual Aid Region VI, which includes the counties of Imperial, Inyo, Mono, Riverside, San Bernardino, and San Diego. The Cal OES Southern Region in Los Alamitos will support the San Bernardino County OA EOC.

4.4 STATE LEVEL

In response to emergency needs and requests from local governments and OAs, the State coordinates mutual aid across mutual aid regions and between regional and state levels while managing its own resources. The State also acts as the primary coordination and communication link between the State and the Federal levels.

4.5 FEDERAL LEVEL

The U.S. Department of Homeland Security (DHS) has designated FEMA to serve as the lead federal agency during disasters and national security emergencies. In a disaster, different federal agencies may be involved in the response and recovery operations. Federal disaster assistance is organized under the concept of Emergency Support Functions (ESFs) as defined in the National Response Framework (NRF). All contact with FEMA and other federal agencies is made

through the OAs during the response phase. During the recovery phase, there may be direct City contact with FEMA and other federal agencies.

4.6 EXTERNAL PARTNERS

4.6.1 NON-GOVERNMENTAL ORGANIZATIONS

Non-governmental organizations (NGOs) play essential roles before, during, and after disasters. NGOs provide a wide range of services such as shelter operations, donations management, food distribution, non-hazardous debris removal, and housing reconstruction support. They provide these services independently or in coordination with Federal, State, and local efforts.

American Red Cross (ARC): Humanitarian organization dedicated to providing emergency assistance, disaster relief, and education. Its core purpose is to help people in crisis by offering life-saving services, such as blood donation drives, disaster response, and supporting military families. The organization also focuses on disaster preparedness, health and safety education, and recovery efforts, aiming to alleviate human suffering and strengthen community resilience. For more information, go to:

https://www.redcross.org/local/california/southern-california.html

National Voluntary Organizations Active in Disaster (NVOAD): Coalition of nonprofit organizations in the U.S. that collaborate to provide disaster relief and recovery services. Its purpose is to coordinate efforts, share resources, and reduce duplication of services, ensuring an efficient and effective response to disasters. NVOAD focuses on providing immediate assistance, long-term recovery, and helping communities prepare for future disasters through member organizations' expertise and volunteer mobilization. For more information, go to:

https://www.nvoad.org

San Bernardino County Voluntary Organizations Active in Disaster (SBCOVOAD): Coalition of nonprofits, faith-based and community organizations, businesses, tribal partners, and government agencies working together to strengthen disaster preparedness, response, and recovery across the largest county in the nation. For more information, go to:

https://sbcovoad.org

Salvation Army: Humanitarian organization focused on providing emergency assistance, disaster relief, and social services to those in need. Its purpose is to alleviate human suffering, promote social justice, and offer hope through programs such as food distribution, shelter, addiction recovery, and disaster response. The Salvation Army works to meet both immediate and long-term needs, serving all individuals and communities. For more information, go to:

https://sanbernardino.salvationarmy.org/san_bernardino_corps

4.6.2 PRIVATE SECTOR

The private sector plays a vital role in the economy and provides essential goods and services that sustain daily life. The City has developed many public-private partnerships and relies on its private sector partners for disaster response and recovery.

According to DHS, the private sector owns and operates approximately 80% of the nation's critical infrastructure, such as energy, telecommunications, transportation, water and wastewater systems, chemical and manufacturing industries, healthcare, and insurance and financial services. The remaining 20% of critical infrastructure is managed by Federal, State, and local governments and typically includes emergency services, public transportation systems, and some water and sewage systems.

Private companies in sectors like food, transportation, healthcare, and logistics provide essential goods and services during and after a disaster. Many of these companies fill critical needs in the community through the donation of goods and resources, in addition to contributing funds to disaster relief and recovery efforts.

4.6.3 SCHOOLS AND ACADEMIC INSTITUTIONS

Schools and academic institutions can serve as centers for recovery, stability, and community support after a disaster, in addition to their traditional educational function. Following a disaster, schools contribute by:

- Serving as shelters for displaced individuals
- Serving as points of distribution for relief supplies
- Providing counseling and mental health services for students and their families
- Reestablishing normalcy for students following disasters

- Providing disaster preparedness training for students and their families

In California, K-12 public schools are required to have disaster plans, conduct periodic drills, and provide educational and training programs to staff and students. Schools and academic institutions should train students and staff in proper emergency response procedures and educate student families on school plans and procedures during and after an emergency (including student release procedures).

4.6.4 FAITH-BASED ORGANIZATIONS

Faith-based organizations (FBOs) play a critical role in all four phases of emergency management and should be incorporated into emergency planning and disaster response. FBOs provide various forms of aid following a disaster and often participate in long-term recovery efforts.

FBOs contribute by:

- Engaging with communities on topics such as household disaster preparedness, hazard mitigation, and basic medical care
- Providing shelter for displaced individuals
- Providing counseling and emotional/spiritual support
- Distributing food, water, and clothing to the community
- Collecting, managing, and distributing donations (cash and material)
- Mobilizing volunteers to assist with tasks such as evacuation, rescue, and basic medical care
- Collaborating with NGOs to ensure aid is distributed fairly and appropriately
- Advocating for the needs of marginalized and vulnerable populations
- Supporting long-term recovery efforts in the form of financial assistance, rehabilitation programs, community cohesion, and rebuilding homes

4.6.5 COMMUNITY INVOLVEMENT

Resilient communities begin with prepared communities. Individuals, families, and caregivers to those with access and functional needs should enhance their awareness of risks and threats, develop household emergency plans that include care for pets and service animals, and prepare emergency supply kits. Individuals can also volunteer in their communities.

Individuals and households play an essential role in emergency management by contributing to community, neighborhood, and family preparedness.

Community members can contribute by:

- Reducing hazards in and around their homes. Hazard reduction actions include making their home earthquake-resistant or storing unanchored objects during high winds. These actions can reduce damage caused by an emergency.
- Preparing an emergency supply kit and household emergency plan. By developing a household emergency plan and assembling disaster supplies before an emergency, people can take care of themselves until assistance arrives. Emergency kits should include supplies for household pets and service animals.
- Monitor emergency communications carefully. Critical information and directions will be released to the public via various media throughout an emergency. By carefully following the directions provided, residents can reduce their risk of injury, keep emergency routes open to response personnel, and reduce the demands on landline and cellular communication.
- Volunteering with an established organization such as CERT. Organizations and agencies with a role in response and recovery are always seeking hardworking and dedicated volunteers. By volunteering with an established volunteer agency, individuals and households become a part of the emergency management system and ensure that their efforts are directed where they are most needed.
- Enrolling in emergency response training courses. Emergency response training, whether basic first aid through the ARC or a more complex course through a local college, will enable residents to take initial response actions required to care for themselves and their households. This allows first responders to focus on higher-priority tasks that affect the entire community.

THIS PAGE IS INTENTIONALLY LEFT BLANK

5. DIRECTION, CONTROL, AND COORDINATION

Direction, control, and coordination define the organizations within the multi-agency coordination system, clarify their roles in emergency operations, and describe how coordination is achieved.

5.1 DIRECTOR OF EMERGENCY SERVICES

The City Manager serves as the Director of Emergency Services and holds full authority over the City's emergency response and recovery efforts. These powers are established in MC § 2.52.100 (Powers and Duties of the Director of Emergency Services).

5.2 CITY EOC

During an emergency or disaster, the City's emergency management functions will be conducted from the primary EOC, located at the Redlands Police Department (1270 W. Park Ave, Redlands, CA 92373). In addition to overseeing City response activities, the EOC serves as the primary link to the San Bernardino County OA and mutual aid partners.

5.3 CITY DEPARTMENT DIRECTION

Each City department operates under its Department Director or designated alternate in preparing for and responding to City emergencies and disasters. When the EOC is activated, department representatives coordinate emergency management functions from the EOC and are empowered to make decisions and allocate resources in accordance with the EOC Action Plan or as directed by the Director of Emergency Services/EOC Director.

5.4 DEPARTMENT OPERATIONS CENTERS

When activated, the management and coordination of department-level response and recovery activities for citywide events, extraordinary emergencies, and disasters will be directed from DOCs.

5.5 LOCAL CONTROL

Local governments manage emergency operations within their jurisdictions in compliance with applicable laws, orders, and regulations. When the City is the Authority Having Jurisdiction (AHJ), it oversees incidents from response to recovery. As outlined in the California Government Code § 8618, the City directs

mutual aid incidents, including personnel and equipment from mutual aid programs. Mutual aid resources remain under the operational control of their respective disciplines and designated Incident Commander (IC).

5.6 ON-SCENE CONTROL

An Incident Commander (IC) from an Incident Command Post (ICP) directs and controls on-scene tactical activities, supporting single incidents, countywide events, complex incidents, or when in an Area Command structure. This on-scene control includes setting tactical objectives and managing resources, including mutual-aid resources. The EOC and DOCs support rather than direct on-scene tactical activities.

5.7 COORDINATION AND INTERFACE

5.7.1 EOC-FIELD COORDINATION AND INTERFACE

EOC-to-field communications typically occur at the Command and General Staff levels and are relayed to the appropriate section or function within the EOC. For example, the Fire-Rescue Branch in the EOC generally communicates directly with the Fire Incident Commander during fire-related incidents.

To support EOC-field coordination and establish a common operating picture, the EOC may consider the following activities to facilitate communication and interface with field operations:

- Assign an EOC representative to the Incident Command Post (ICP)
- Have an EOC representative attend ICP operations briefings
- Have an ICP representative attend EOC operations briefings
- Coordinate and share EOC Action Plans with the ICP
- Coordinate and share ICP Incident Action Plans (IAPs) with the EOC
- Share EOC Situation Reports with the ICP
- Share ICP Situation Reports with the EOC

5.7.2 EOC-DOC-FIELD COORDINATION AND INTERFACE

Effective emergency response depends on coordination across all SEMS levels. In major incidents, the City EOC may activate to manage the broader response, while DOCs support field command posts when multiple incidents strain departmental

resources. Field ICs communicate with their respective DOCs or directly with the EOC Operations Section, based on the nature of the incident. DOCs maintain situational awareness and may activate independently to manage multiple incidents, under the direction of the Department Director. The City EOC facilitates communication with ICPs and DOCs as needed.

5.7.3 OPERATIONAL AREA COORDINATION

OA coordination is maintained through each jurisdiction's Emergency Manager, who serves as the primary link between local EOCs and the San Bernardino County OES, which operates the OA EOC. The OA supports countywide coordination by gathering and sharing situational information, facilitating resource requests, and maintaining consistent communication across jurisdictions. Member agencies use the Multiagency Coordination System to prioritize incidents and share resources, with situation reporting and resource coordination managed through the OA's WebEOC platform.

5.7.4 MULTIAGENCY COORDINATION

Multiagency coordination enables all levels of government to establish incident priorities and allocate resources across multiple incidents or jurisdictions. The Multiagency Coordination System (MACS) integrates personnel, procedures, and communication systems to support unified decision-making.

MAC Groups may include:

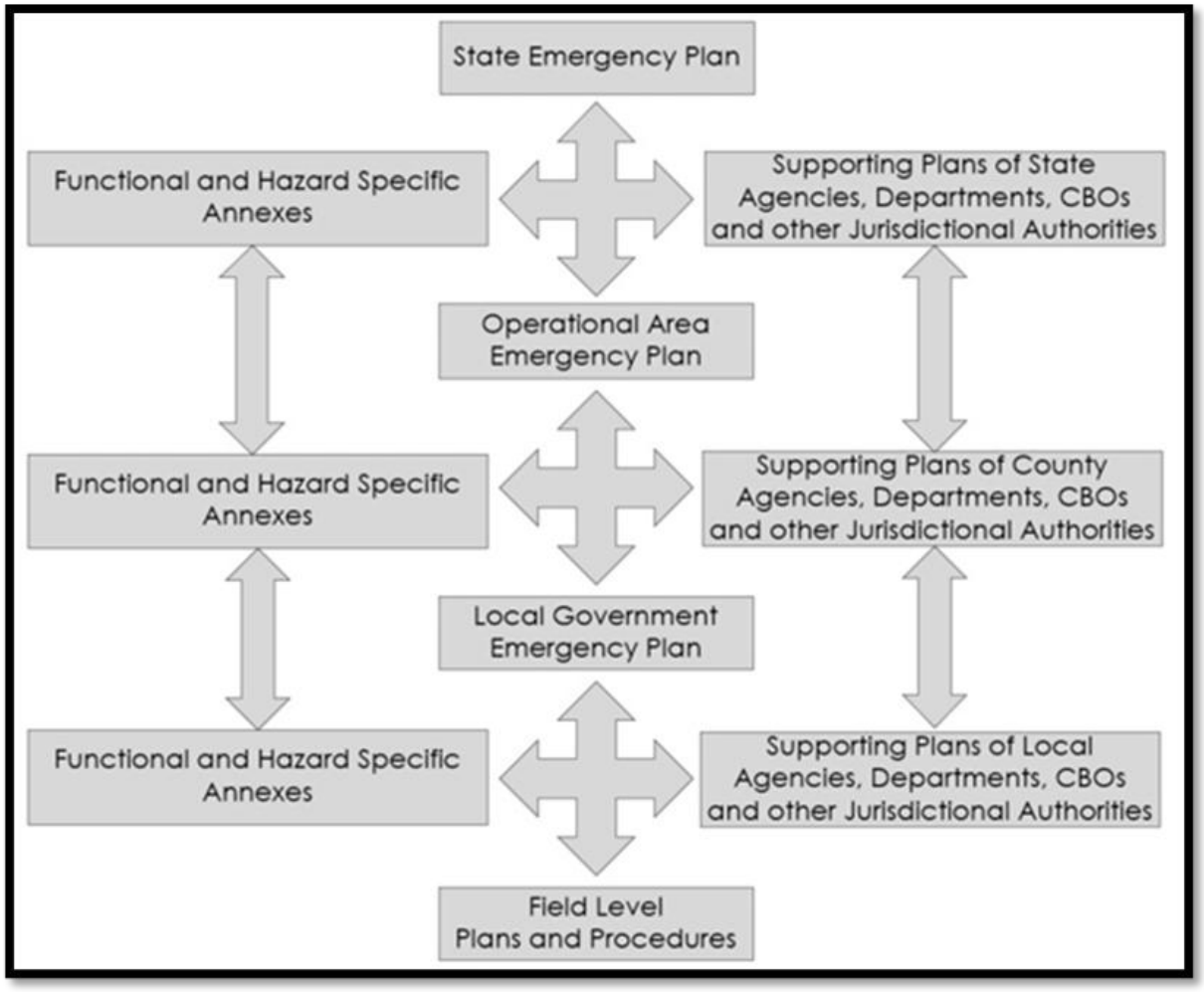
- Representatives from the City departments
- Representatives from outside agencies including special districts, volunteer agencies, and private partners
- Coordination with agencies not represented in the EOC
- Departments and agencies in the EOC action planning
- OA Mutual Aid Coordinators and mutual aid providers

The OA EOC may coordinate conference calls before or during emergencies. In this case, the OA jurisdictions may serve as a MACS Group to coordinate situational information and share resources. The City most often participates in a MAC System or Group through OA emergency management coordination.

5.7.5 EMERGENCY PLAN COORDINATION

The City EOP functions within a broader planning framework that supports emergency management at the local and regional levels. Graphic 5.7.5 below illustrates this coordinated framework.

Graphic 5.7.5: Emergency Plan Coordination

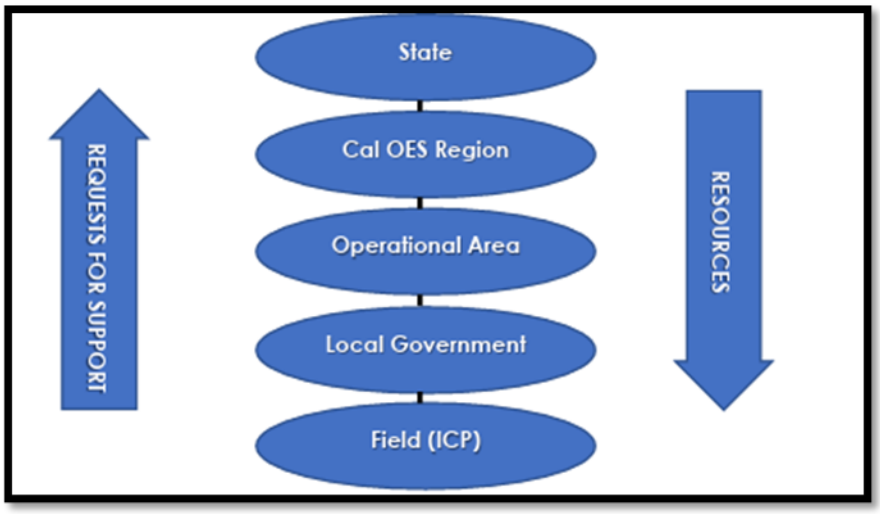


Source: California State Emergency Plan, 2024

5.7.6 EMERGENCY MANAGEMENT COORDINATION

The City's emergency management system operates within the broader SEMS framework, which facilitates coordination of information and resources at the local and regional levels. Graphic 5.7.6 below illustrates this coordinated framework.

Graphic 5.7.6: Emergency Management Coordination



Source: California State Emergency Plan, 2024

5.7.7 STATEWIDE EMERGENCY MANAGEMENT COORDINATION

Cal OES operates three administrative regions—Inland (Sacramento), Coastal (Fairfield), and Southern (Los Alamitos)—which coordinate information and resources across SEMS levels to support local response. These regions represent local perspectives and provide a Cal OES presence throughout all phases of emergency management. The City is part of the Cal OES Southern Region. Graphic 5.7.7 below illustrates the Cal OES Regions.

Graphic 5.7.7: Cal OES Regions

Source: Cal OES

6. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

The City EOC serves as the central hub for collecting, verifying, analyzing, and disseminating emergency information with internal departments, the OA, adjacent jurisdictions, and supporting agencies during City-related incidents. The City is not responsible for managing situational data for emergencies occurring outside its jurisdiction.

Prior to EOC activation, the City may receive alerts and warnings from multiple sources, including the San Bernardino County OES, the San Bernardino County Sheriff's Department Dispatch Center, CONFIRE, the California State Warning Center (CSWC), City departments, neighboring municipalities, utility providers, and the National Weather Service (NWS).

Once activated, the EOC Planning & Intelligence Section leads the collection, evaluation, display, and distribution of incident information, including situational status and resource status. This section supports decision making across the EOC by providing accurate intelligence, anticipating operational developments, producing situation forecasts, and maintaining a common operating picture for all EOC sections.

6.1 OBJECTIVES

Objectives of the information collection, analysis, and dissemination function include, though are not limited to, the following:

- Inform the decision to proclaim local emergencies
- Collect and analyze initial situation reports, including safety conditions and damage assessments
- Display incident data using maps, status boards, and other visual tools within the EOC
- Develop and maintain charts and logs tracking incident status and available resources (personnel, equipment, vehicles, and teams)
- Disseminate intelligence updates to the EOC Director, Management Staff, and General Staff

- Coordinate Geographic Information Systems (GIS) support for mapping and incident documentation
- Prepare and distribute summary reports on safety conditions and damage assessments to EOC Sections, the San Bernardino County EOC, Cal OES, and FEMA
- Document damage levels and develop preliminary financial loss estimates
- Provide situational awareness and planning support to EOC Sections and DOCs
- Develop the City's EOC Action Plan, incorporating input from all sections.
- Coordinate and prepare the City's After-Action Report and Corrective Action Plan following EOC demobilization
- Initiate post-disaster recovery planning and support the transition to a formal Recovery Organization
- Maintain accurate and complete documentation of all EOC activities; ensure record preservation and submit required reports to the San Bernardino County OES, Cal OES, and FEMA
- Identify and coordinate technical experts for specialized topics requiring subject matter expertise
- Provide technical and informational support to the EOC Director for presentations to the City Council, Policy Group, public meetings, and media briefings
- Support mutual aid resource requests and deployments

6.2 INFORMATION COLLECTION

6.2.1 OVERVIEW

Emergency incident information may originate from the following sources:

- Operations Section Branches, including reports from field personnel, DOCs, dispatch centers, and external partners
- Media (television, radio, and print)
- Social media platforms

- Field Observers assigned by the EOC
- Damage Assessment and Damage Inspection Teams
- Situation reports from County, State, and Federal agencies
- Agency representatives assigned to the EOC
- Redlands Emergency Communications Group
- Community-based and neighborhood groups (e.g., CERT, Neighborhood Watch, Neighborhood Associations)
- Preparedness partners such as schools, hospitals, and non-governmental organizations (NGOs)

6.2.2 PRE-EOC ACTIVATION

Prior to EOC activation, incident or situational information may be received from a variety of sources, including:

- San Bernardino County OES
- San Bernardino County EOC
- San Bernardino County Sheriff's Department
- San Bernardino County Fire Protection District
- Consolidated Fire Agencies (CONFIRE)
- Los Angeles Joint Regional Intelligence Center (JRIC)
- California State Warning Center (CSWC)
- City departments and field personnel
- Neighboring jurisdictions
- Utility providers and critical infrastructure partners
- National Weather Service (NWS)

Information is evaluated for accuracy and relevance, then shared with appropriate City officials or departments for situational awareness and potential response coordination.

6.2.3 EOC ACTIVATION

During an EOC activation, the Planning & Intelligence Section is responsible for collecting, analyzing, and displaying accurate and timely information related to the current situation and resource status. This EOC Section ensures that safety and damage assessment data is gathered, compiled, and reported promptly to all EOC Sections, the San Bernardino County OA, and the Cal OES Regions.

The Planning & Intelligence Section coordinates the development of the EOC Action Plan, incorporating input from the EOC Management Section and Section Chiefs to establish operational priorities and guide response activities.

Additionally, the Planning & Intelligence Section manages the Documentation Unit, which is tasked with maintaining detailed records of the emergency response and ensuring those records are preserved for after-action reporting, cost recovery, and historical reference.

The City EOC uses Microsoft platforms (e.g., SharePoint and Teams) for internal incident and resource tracking; WebEOC is used for coordination with the San Bernardino County EOC.

6.3 ANALYSIS AND DISSEMINATION

Analysis: The analysis function transforms raw incident data into actionable intelligence by identifying patterns, assessing impacts, and supporting decision-making across the EOC.

Dissemination: The dissemination function ensures timely, accurate, and targeted delivery of critical information to decision makers, responders, and stakeholders during an emergency.

Once verified, validated, and organized, emergency incident information is disseminated by the EOC Planning & Intelligence Section through multiple channels and formats, including:

- **Internal:** EOC briefings, EOC Action Plans, situation reports, situation displays, internal communications, and EOC Section updates.
- **External:** WebEOC/CalEOC updates, San Bernardino County OA Situation Reports and reporting forms, shared EOC Action Plans, and County emergency management staff assigned to the City EOC.

- **Public:** The PIO coordinates public messaging through the Joint Information System (JIS) or Joint Information Center (JIC) to ensure verified information reaches the public.

THIS PAGE IS INTENTIONALLY LEFT BLANK

7. COMMUNICATIONS

7.1 PUBLIC ALERT AND WARNING

Alert and warning refer to the systems and processes used by government agencies to notify partner organizations and the public of imminent threats or extraordinary hazards. Dependent upon the nature of the threat and the population at risk, alert and warning can originate at any level of government. Protection of life and property is dependent upon timely dissemination of warning and emergency information to the populations in threatened areas.

The City is responsible for alerting and warning within City limits. There are various means and methods whereby an alert or warning may originate and be disseminated to the City and/or San Bernardino County.

7.1.1 RAVE ALERT

The City uses Rave Alert as its emergency mass notification system. The system enables City officials to distribute time-sensitive alerts and public safety information during incidents such as wildfires, floods, hazardous materials incidents, evacuations, and other emergencies.

Notifications, which may be sent as phone calls, text messages, or emails, typically include protective action guidance and other critical information intended to help City residents respond to developing situations.

The Redlands Police Department Communications Unit and Redlands Fire Department/Emergency Management have the ability to send out Rave Alert notifications within City limits.

City residents and employees can register for Rave Alert at https://www.smart911.com/smart911/ref/login.action?pa=cityofredlands.

7.1.2 TELEPHONE EMERGENCY NOTIFICATION SYSTEM

San Bernardino County uses the Telephone Emergency Notification System (TENS), also known as the Reverse 9-1-1 Public Warning System, to deliver rapid emergency notifications to the public. The system alerts County residents to life-threatening incidents such as wildfires, floods, hazardous materials incidents, and other emergencies. The system may provide time-sensitive protective action instructions

including evacuation orders, shelter-in-place directives, or other emergency guidance.

The system enables public safety officials to issue targeted notifications to specific geographic areas based on geocoded addresses and the County's street network. This capability allows alerts to be distributed during both localized and large-scale emergencies.

TENS delivers high-speed notifications through voice and text messaging and is compatible with TDD/TTY devices to support accessible communications.

City residents and employees can register for TENS at https://www.smart911.com/smart911/login.action?lpse=1.

7.1.3 INTEGRATED PUBLIC ALERT AND WARNING SYSTEM

IPAWS is a national FEMA-managed system that allows authorized agencies to issue emergency alerts through multiple channels, including the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), and NOAA Weather Radio. In San Bernardino County, the components of IPAWS are accessed through the TENS portal and require special codes, available through the San Bernardino County Sheriff's Department and San Bernardino County OES, in order to launch messages using its component technologies.

The City may request IPAWS activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.4 EMERGENCY ALERT SYSTEM

7.1.4.1 OVERVIEW

The Emergency Alert System (EAS) enables Federal, State, and local governments to communicate with the public via commercial broadcast stations. Operated voluntarily by broadcasters under Federal Communications Commission (FCC) regulations, EAS disseminates critical emergency information. Message priorities under Part 73.922(a) of the FCC's rules are as follows:

- Priority One: Presidential Messages (live)
- Priority Two: EAS OA (Local) Programming
- Priority Three: State Programming

- Priority Four: National Programming and News

California has 30 EAS OAs within radio reception range of EAS stations serving the area. The State message priorities are as follows:

- Priority One: Immediate action required to save lives
- Priority Two: Property protection and urgent public instructions
- Priority Three: General public information

7.1.4.2 SAN BERNARDINO COUNTY

EAS messages are broadcast in San Bernardino County to all local broadcasters, special districts, and businesses with over 100 employees. Local EAS stations authenticate requests before broadcasting. Authentication details are not released to the public. Emergencies warranting alerts include natural disasters, public safety threats, and hazardous materials incidents.

EAS activation in San Bernardino County can be authorized by the San Bernardino County Sheriff's Department and San Bernardino County OES.

The local EAS stations for southwestern San Bernardino County are:

- Primary Station (LP1): KFRG-95.1 FM
- Alternate Station (LP2): KGGI-99.1 FM

The City may request EAS activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.5 WIRELESS EMERGENCY ALERTS

Wireless Emergency Alerts (WEA) deliver text messages to compatible cellular phones in affected areas, warning users of hazards and providing brief instructions. WEA is enabled by default and does not require opt-in.

WEA messages have the following character limits:

- 360 characters (4G LTE and newer networks)
- 90 characters (3G and older networks)

When sent via IPAWS, alerts are transmitted to cell carriers, which broadcast them from towers in the alert zone. Exact reach is unpredictable due to factors like:

- Geography affecting reception

- Buildings limiting signal penetration
- Device status (powered off or out of battery)
- Towers lacking backup power during outages
- Antenna type (directional vs. omnidirectional) and signal strength

The City may request WEA activation through the San Bernardino County Sheriff's Department and San Bernardino County OES.

7.1.6 CALIFORNIA STATE WARNING CENTER

The California State Warning Center (CSWC) is the official State level point of contact for emergency notifications. The CSWC maintains contact with OA Warning Points, state agencies, federal agencies and the National Warning Center.

- **Notifications received by CSWC:** Local governments and OAs notify the CSWC of emergencies that affect their community in accordance with existing laws, protocols or when State assistance is requested or anticipated.
- **Earthquake Notifications:** The CSWC receives notifications of earthquakes from the California Integrated Seismic Network (CISN), National Earthquake Information Center (NEIC), and the United States Geological Survey (USGS).
- **Weather Notifications:** Notification of severe weather is received from the NWS San Diego Office.
- **Energy Notifications:** The California Independent Systems Operator (California ISO) monitors the State's power grids.
- **Hazardous Materials, Oil Spill Release Notifications:** In accordance with State law, CSWC will be notified of any release or threatened release of hazardous materials.

The CSWC is responsible for informing, communicating, alerting, and notifying local government, OAs, State officials, and the Federal government of emergencies. The CSWC is equipped with telephone, data, and radio systems, including CALWAS, CLETS, NWS Weather Radio (NWR), Emergency Digital Information Service (EDIS), and Dialogic Emergency Notification System (DENS). Most of these systems are used on a day-to-day basis; others are available for use in an emergency, as conditions require.

- **CALWAS:** The CSWC maintains the California Warning System (CALWAS) to communicate with Cal OES Regional Offices and County Warning Points during an emergency. CALWAS is part of the National Warning System (NAWAS).
- **CLETS:** The California Law Enforcement Telecommunications System (CLETS) is a high-speed message switching system that provides law enforcement and criminal justice agencies with the capability of obtaining information directly from Federal, State, and local computerized information files. In addition, the system will provide fast and efficient point-to-point delivery of messages between agencies.
- **OASIS:** Cal OES leases transponder space from a commercial satellite operator and operates a satellite communications system known as Operational Area Satellite Information System (OASIS). This system serves as one of the back-up and redundancy systems and allows public safety agencies to exchange disaster intelligence and resource requests when the Public Switched Telephone Network (PSTN) fails. In the event of PSTN failure, OASIS is the primary back-up, providing voice and internet connectivity with the CSWC, Cal OES REOCs, key State agencies, and each OA.

7.1.7 NATIONAL WEATHER SERVICE

National Weather Service (NWS) provides weather forecasts and warnings to the nation. The City and southwestern San Bernardino County receive notifications from the San Diego Forecast Office.

NWS transmits continuous weather information for the San Bernardino County area on 162.450 MHz. The NWS severe weather broadcasts are preceded with a 1050 MHz tone that activates weather monitor receivers equipped with decoders. The NWS can also access NAWAS to announce severe weather information, which is disseminated to the county warning points using the CALWAS system.

The levels of notifications that the NWS issues include the following:

- **Outlook:** Indicates the potential for hazardous weather over the coming days, intended to provide advance awareness with low certainty and no immediate action required.
- **Statement:** Provides additional information, updates, or clarification about ongoing or recent weather conditions.

- **Watch:** Indicates that conditions are favorable for a specific hazard to develop, meaning individuals should remain alert and prepared to take action.
- **Advisory:** Indicates that weather conditions that may cause inconvenience or minor impacts, requiring caution but typically not posing a significant threat to life or property.
- **Warning:** Indicates that a hazardous event is imminent or occurring, requiring immediate protective action.

7.1.8 ROUTE ALERTING AND DOOR-TO-DOOR CANVASSING

The City may use route alerting and door-to-door canvassing to alert and notify the public. Route alerting is commonly used in small-scale emergencies or rapidly evolving situations within a defined area. It involves emergency officials driving or walking through the affected zone to inform residents of the situation and recommended actions. This can be done door-to-door or via public address systems on police or fire vehicles.

While effective, especially when other systems are unavailable, route alerting depends on resource availability and can be time-consuming. It is typically used in localized settings such as neighborhoods, apartment complexes, mobile home parks, hotels, and college campuses. Route alerting can also serve as a supplement to other alert and warning methods.

7.2 COMMUNICATION SYSTEMS

7.2.1 TELEPHONES

The City EOC has one dedicated VoIP phone, with additional VoIP phones available in the room through the Redlands Police Department. Conference call phones and numbers can be provided as needed. Requests for any additional telecommunications support should be routed to the EOC Logistics Section, Communications Unit.

7.2.2 CELLULAR PHONES

The City maintains cellular service through multiple providers, and City-issued cell phones are assigned to staff for use in the EOC and during emergency operations. These phones support voice, text, and data and serve as a backup to landline and

radio systems. During major incidents, network congestion may occur, so staff should use text messaging when possible to improve reliability.

7.2.3 EMAIL

Email is a redundant method of communication between the OA EOC and the City EOC due to the number of reporting jurisdictions and the quantity of documentation provided. Like cellular telephones, if other primary means of data or voice communications fail, then email should be considered a sufficient back-up. Before using email, however, personnel should confirm that the intended recipient(s) has access to and is checking their email. Critical information should never be sent over email unless confirmation exists that the intended recipient is receiving the messages.

7.2.4 800 MHZ RADIOS

The City EOC has connectivity to San Bernardino County's 800 MHz system, which provides access from the EOC to field personnel (e.g., fire, police, public works, public utilities, etc.) and potentially to mutual aid partners. During an emergency, City radios should be limited to emergency radio traffic only.

7.2.5 SATELLITE TELEPHONES

The City has four portable satellite phones for communicating with other cities and agencies belonging to the emergency managers talk group. Satellite phones use a geostationary satellite above Earth as a repeater and serve as backup communication if other systems fail.

Two units are assigned to the Redlands Fire Department (Fire Chief and Emergency Management), and two units are assigned to the Redlands Police Department (Communications Unit and Mobile Command Post).

7.2.6 REDLANDS EMERGENCY COMMUNICATIONS GROUP

The Redlands Emergency Communications Group (RECG), also known as the Radio Amateur Civil Emergency Service (RACES), consists of volunteer amateur radio operators who are committed to assisting with emergency communications in times of disaster. RECG is managed by the Fire Department and provides auxiliary communications support for EOC operations, field operations, and City departments.

7.2.6.1 SAN BERNARDINO COUNTY RACES

San Bernardino County maintains a cadre of RACES volunteers and radio base stations to ensure communications between the OA EOC and various locations can be maintained. Individual operators may have their own base stations that can also be dispatched at the discretion of the OA EOC. Emergency information can be communicated through RACES operators to any location where an operator is dispatched (e.g., mutual aid EOCs, Incident Command Posts, shelters, staging areas, etc.). Emergency information of any sort may be communicated through a ham radio operator.

While operating in a RACES capacity, stations and amateurs registered with the local RACES organization may not communicate with amateurs who are not operating in that capacity.

7.2.7 INLAND SOCAL 211

The 211 system is an FCC-designated, three-digit number that connects the public to community, health, and social service resources; it is not a dispatch line like 911, 988, or 311, though it can support emergencies by providing verified information and referrals. Inland SoCal 211, operated by the Inland Southern California United Way, offers 24/7 access to services and helps San Bernardino County residents during emergencies in coordination with the American Red Cross (ARC) and other partners.

7.2.8 RELAY SERVICES

California Connect provides a statewide telecommunications relay service that enables California residents with speech, hearing, vision, mobility, or cognitive disabilities to connect using functional equivalent equipment and services. The service offers voice-to-text, text-to-voice, and other assistive communication options to ensure accessible and reliable communication during emergencies and routine operations. This service is available by dialing 7-1-1.

7.2.9 WEBEOC

San Bernardino County OES uses WebEOC as its crisis information management system. WebEOC is a web-based platform that enables secure, real-time information sharing and resource coordination during disasters and emergencies.

The City uses WebEOC to:

- Share situational status information with San Bernardino County
- Coordinate resource requests with San Bernardino County

7.3 PUBLIC INFORMATION

7.3.1 CITY BROADCAST

The City operates a broadcast channel called Redlands TV, which features live and recorded meetings, community programming, and special events coverage.

Redlands TV is available to cable television subscribers through Spectrum cable (Channel 3) or Frontier cable (Channel 35) services and is also hosted online at https://www.redlands.gov/redlands-tv.

7.3.2 SOCIAL MEDIA

The City utilizes its website and social media platforms to reach the public. In an emergency or disaster, the City EOC will post information on these accounts and monitor these accounts for messages and information from the public.

- City Website: https://www.redlands.gov
- Facebook: https://www.facebook.com/cityofredlands
- Instagram: https://www.instagram.com/cityredlands
- X (formerly Twitter): https://x.com/cityofredlands

7.3.3 MEDIA BRIEFINGS AND PUBLIC MEETINGS

The City may hold media briefings and community meetings before, during, and after emergencies to provide essential updates. Accessibility measures will include sign language interpreters, large-print materials, and translation services.

During EOC activations, the Public Information Officer (PIO) will develop key messages, anticipate public questions, and highlight response and recovery efforts.

THIS PAGE IS INTENTIONALLY LEFT BLANK

8. MUTUAL AID AND RESOURCE MANAGEMENT

8.1 MUTUAL AID OVERVIEW

California's basis for mutual aid is the California Civil and Defense Master Mutual Aid Agreement (MMAA), through which the State, its agencies, political subdivisions, public agencies, and federally recognized tribes agree to support one another when local resources are insufficient. The MMAA requires signatories to provide assistance without expectation of reimbursement, although federal or State funding may reimburse eligible costs. Assistance provided under other agreements, memoranda, or contracts is governed by the terms of those documents.

Mutual aid requests follow established, discipline-specific procedures and are routed through designated mutual aid coordinators, who manage resource requests within their areas and elevate them to the next level of government when necessary.

The City of Redlands participates in California's mutual aid system to ensure rapid access to additional personnel and resources during major incidents and to provide reciprocal support to neighboring jurisdictions when their needs exceed local capacity. Through this system, Redlands benefits from statewide surge capability and, when it deploys resources to assist others, the City is eligible to recover its allowable response costs plus any approved administrative overhead in accordance with California mutual aid reimbursement policies.

8.2 MUTUAL AID AGREEMENTS

Mutual aid agreements are fundamental to effective emergency management, enhancing resource availability and improving the City's capacity to respond to and recover from disasters.

Mutual aid assistance within California is provided under the following authorities:

- California Civil and Defense Master Mutual Aid Agreement
- California Fire and Rescue Mutual Aid Plan
- California Urban Search and Rescue Mutual Aid Plan
- California State Mutual Aid Pre-Position Program

- California Law Enforcement Mutual Aid Plan
- California Search and Rescue Mutual Aid Plan
- California Coroner Mutual Aid Plan
- California Public Health and Medical Assistance
- California Emergency Managers Mutual Aid (EMMA)
- California Public Works Mutual Aid Agreement

Mutual aid assistance between states may be provided under the following authorities:

- Emergency Management Assistance Compact (EMAC)
- Robert T. Stafford Disaster Relief and Emergency Assistance Act

8.3 CALIFORNIA MUTUAL AID FRAMEWORK

8.3.1 STATE MUTUAL AID PROVISIONS

State agencies may provide mutual aid—personnel, equipment, and other resources—to support political subdivisions during a Local Emergency, under existing mutual aid agreements, or at the Governor's direction. This authority enables the City to receive direct State assistance when local and County resources are exceeded.

8.3.2 MUTUAL AID CHARGES AGAINST THE STATE

In the absence of a State of War Emergency or State of Emergency, the cost of extraordinary services incurred by political subdivisions in executing mutual aid agreements constitutes a legal charge against the State when approved by the Governor under orders and regulations issued pursuant to California Government Code § 8567. This provision allows the City to receive State reimbursement for eligible extraordinary mutual aid costs incurred outside a declared state emergency.

8.3.3 CALIFORNIA MUTUAL AID PROGRAMS

The State's mutual aid programs, which are coordinated by Cal OES and the Emergency Medical Services Authority (EMSA), are summarized in Table 8.3.3 on the next page.

Table 8.3.3 California Mutual Aid Programs

CALIFORNIA MUTUAL AID PROGRAMS MUTUAL AID SYSTEMS AND CHANNELS OF STATEWIDE MUTUAL AID COORDINATION			
COORDINATED BY CAL OES			COORDINATED BY EMSA
Fire & Rescue	**Law Enforcement**	**Emergency Management**	**Disaster Medical & Health**
Fire & Rescue Mutual Aid	Coroner Mutual Aid	Public Works Mutual Aid	Medical Mutual Aid
Urban Search & Rescue Mutual Aid	Law Enforcement Mutual Aid	California Water/Wastewater Agency Response Network (CalWARN)	
	Search & Rescue Mutual Aid (non-urban)	Emergency Managers Mutual Aid (EMMA)	

8.3.4 CALIFORNIA MUTUAL AID REGIONS

The State of California is divided into three Administrative Regions and six Mutual Aid Regions to coordinate mutual aid. The City is in Mutual Aid Region VI within the Southern Administrative Region.

A Mutual Aid Region is a subdivision of Cal OES established to facilitate coordination of mutual aid and emergency operations within an area of the State consisting of two or more county OAs. An OA is an intermediate level of the state emergency services organization consisting of a county and all political subdivisions within that county.

Cal OES Mutual Aid and Administrative Regions are illustrated in Graphic 8.3.4 on the next page.

Graphic 8.3.4 Cal OES Mutual Aid and Administrative Regions

Source: Cal OES

8.3.5 MUTUAL AID COORDINATION

Mutual aid systems work through designated Mutual Aid Coordinators at the local agency, OA, regional, and State levels. Mutual Aid Coordinators receive requests, coordinate the provision of resources within their designated geographic areas of responsibility, and send unfilled requests to the next level of coordination.

8.3.6 LOCAL CONTROL

The City will retain command of incidents within its jurisdiction that require mutual aid, consistent with California Government Code § 8618:

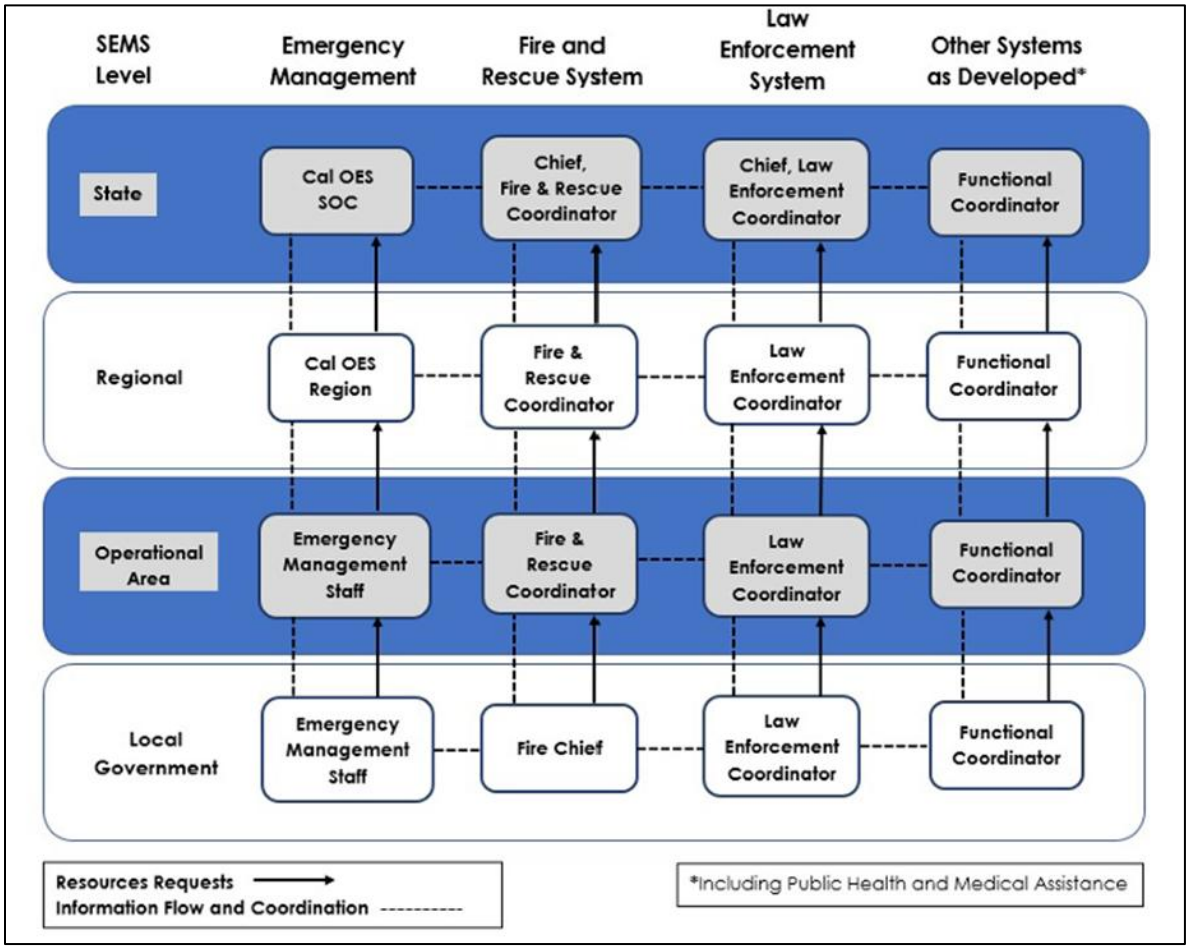
"Unless otherwise expressly provided by the parties, the responsible local official in whose jurisdiction an incident requiring mutual aid has occurred shall remain in charge at such incident, including the direction of personnel and equipment provided to him through mutual aid."

8.3.7 DISCIPLINE-SPECIFIC MUTUAL AID COORDINATION

The statewide mutual aid system incorporates several discipline-specific mutual aid systems, including Fire and Rescue, Law Enforcement, and Emergency Management. Fire and Rescue Mutual Aid Coordinators and Law Enforcement Mutual Aid Coordinators are designated at the OA, regional, and State levels to support mutual aid coordination during both routine and large-scale public safety incidents. Regional Disaster Medical Health Coordinators are also assigned within each mutual aid region to coordinate medical mutual aid. Mutual aid requests outside these discipline-specific systems are coordinated through EMMA by emergency management personnel at the local, OA, regional, and State levels.

Discipline-specific mutual aid systems are illustrated in Graphic 8.3.7 below.

Graphic 8.3.7 Discipline-Specific Mutual Aid Coordination



Source: Cal OES

8.4 CITY MUTUAL AID PARTICIPATION

The City participates in multiple statewide, regional, and industry mutual aid systems. Participation in these **State systems** is coordinated by the City departments listed in Table 8.4.

Table 8.4 California Mutual Aid Program Participation

CA MUTUAL AID PROGRAM	RESPONSIBLE CITY DEPARTMENT
Fire & Rescue	Fire Department ▪ On-Duty Battalion Chief
Law Enforcement	Police Department ▪ Watch Commander
Public Works	Facilities & Community Services Department ▪ Director
Utilities (Water & Electric)	Municipal Utilities & Engineering Department ▪ Director
Emergency Managers Mutual Aid (EMMA)	City Manager's Office / Fire Department ▪ City Manager, Assistant City Manager, Fire Chief, or their designee

8.4.1 CITY MUTUAL AID COORDINATION

Participation in all mutual aid programs, including **statewide, regional, and industry mutual aid systems**, is coordinated by the City departments listed in Table 8.4.1.

Table 8.4.1 City Mutual Aid Coordination

MUTUAL AID PROGRAM	RESPONSIBLE CITY DEPARTMENT
American Water Works Mutual Aid (via CalWARN)	Municipal Utilities & Engineering Department
California Master Mutual Aid Agreement (MMAA)	City Manager's Office / Fire Department
California Utilities Emergency Association (CUEA) **Mutual Aid**	Municipal Utilities & Engineering Department
California Water/Wastewater Agency Response Network (CalWARN)	Municipal Utilities & Engineering Department
Coroner Mutual Aid	Police Department (via San Bernardino County Sheriff's Department)
Edison Electric Institute Mutual Aid	Municipal Utilities & Engineering Department (as coordinated through SCE)
Emergency Managers Mutual Aid (EMMA)	City Manager's Office / Fire Department
Emergency Response Network of the Inland Empire (ERNIE) **Mutual Aid**	Municipal Utilities & Engineering Department, and Fire Department Emergency Management Division
Law Enforcement Mutual Aid (LEMA)	Police Department
Medical Mutual Aid	Fire Department (via CONFIRE Communications Center)

Public Health Mutual Aid	Fire Department (via SBCO DPH)
Public Power Mutual Aid	Municipal Utilities & Engineering Department (as coordinated through SCE)
Public Works Mutual Aid	Facilities & Community Services Department
Search and Rescue Mutual Aid	Police Department
Urban Search and Rescue Mutual Aid	Fire Department
Western Region Mutual Assistance Group (WRMAG)	Municipal Utilities & Engineering Department (as coordinated through SCE)

8.4.2 EMERGENCY RESPONSE NETWORK OF THE INLAND EMPIRE

The City is a member of the Emergency Response Network of the Inland Empire (ERNIE), which was established in 2006 and operates within Riverside and San Bernardino Counties. ERNIE is a consortium of public agencies that facilitates preparedness, response, and recovery for local and regional disasters and supports continuity of critical public services. Through a formal mutual assistance agreement, ERNIE member agencies provide personnel, equipment, and other resources to jurisdictions when incidents exceed local capabilities, consistent with applicable State and Federal requirements, and support training, interoperable communications, reimbursement documentation, and After-Action Report/ Improvement Plan (AAR/IP) development.

8.5 EMERGENCY MANAGEMENT ASSISTANCE COMPACT

The Emergency Management Assistance Compact (EMAC) is a congressionally ratified interstate mutual aid agreement that provides the structure and procedures for states and territories to request and render emergency assistance. California is a member of EMAC. Once the Governor proclaims a State of Emergency, California may request and receive assistance from other EMAC member states. The Director of Cal OES, supported by the State's EMAC Coordinator, is responsible for facilitating EMAC requests and deployments.

The City may request or receive assistance through the Emergency Management Assistance Compact (EMAC) when coordinated by Cal OES, which serves as the State's EMAC authority.

8.6 RESOURCE MANAGEMENT OVERVIEW

The City will manage local and mutual aid resources in accordance with SEMS and NIMS.

Resource management during incidents will include:

- **Identification and Typing of Resources** – City departments will maintain current inventories of personnel, equipment, facilities, and supplies. Where applicable, inventories will be kept consistent with Cal OES and FEMA resource typing standards.
- **Request and Coordination** – City requests for **non-mutual-aid resources** go through the City EOC and are coordinated by the EOC Logistics Section. **Mutual aid requests** move through the appropriate discipline-specific mutual aid system and are coordinated by Mutual Aid Coordinators at the City, County, regional, and State levels.
- **Resource Tracking** – **Non-mutual-aid resources** are tracked by the EOC using established EOC resource management tools for status, location, and assignment. **Mutual aid resources** are tracked within the respective discipline-specific mutual aid system using that system's established tracking processes.
- **Demobilization and Return** – **Non-mutual-aid resources** are demobilized through the EOC and released as soon as they are no longer required, then returned in the condition received unless otherwise specified. **Mutual aid resources** are demobilized through their respective mutual aid systems and released according to that system's established procedures, with resources returned in the condition received unless otherwise specified.
- **Documentation** – Resource requests and utilization will be documented by the requesting department and the City EOC to ensure accountability and to support reimbursement through programs such as the California Disaster Assistance Act, the California Fire Assistance Agreement, and applicable federal reimbursement programs.

8.6.1 RESOURCE PRIORITIZATION

When resource availability is limited, priority will be given to:

1. Protection of life
2. Protection of property and the environment
3. Incident stabilization

When the City EOC is not activated, City resource allocation decisions will be managed by the appropriate City department, while mutual aid resource allocation decisions will be coordinated through the appropriate Mutual Aid Coordinator.

When the City EOC is activated, City resource allocation decisions will be coordinated by the EOC Director in consultation with the Operations Section and Logistics Section Chiefs, while mutual aid resource requests and allocations will continue to be processed through the applicable mutual aid system and its designated Mutual Aid Coordinators.

8.6.2 RESOURCE ORDERING AND TRACKING

The City will order, assign, and track City resources using local systems and processes. Mutual aid resources will be requested, coordinated, and tracked through the applicable discipline-specific mutual aid systems and their designated Mutual Aid Coordinators.

When City resources are insufficient or additional support is required, the City EOC will submit and track resource requests through the County's WebEOC platform, which provides centralized, real-time coordination of personnel, equipment, and supplies.

The City remains accountable for resources not tracked by other entities and will monitor the following for each resource:

- Current status (available, assigned, out of service)
- Location and mission assignment
- Estimated time of arrival and assignment duration

Resource tracking may also be supported through:

- Digital EOC (City EOC Microsoft Teams account)
- Incident/EOC Check-In Lists

- Resource Request Message Forms
- Resource Status Cards (T-Cards)
- Other approved EOC tracking tools or technology

8.6.3 INTEGRATION WITH PRIVATE SECTOR AND NON-GOVERNMENTAL ORGANIZATIONS

The City may also access resources from the private sector, non-governmental organizations, and community partners to supplement operations. Examples include:

- Pre-approved or contracted vendors for emergency supplies, fuel, transportation, etc.
- The American Red Cross and other partners for sheltering and feeding
- Faith-based organizations, businesses, and volunteer groups within the City that support emergency response and recovery

8.6.4 RESOURCE DEMOBILIZATION

- **City (non-mutual-aid) resources** are released promptly when no longer required and demobilized through the City's internal processes, coordinated by the Logistics Section in consultation with the Operations Section.
- **Mutual aid resources** are released when no longer required and demobilized through the same mutual aid channels used for their request, in coordination with the appropriate Mutual Aid Coordinator.
- **All released resources** are documented, and any repair or replacement agreements are managed by the EOC Finance & Administration Section. Resources are returned to their point of origin in the condition received unless otherwise stated.

THIS PAGE IS INTENTIONALLY LEFT BLANK

9. CONTINUITY OF GOVERNMENT

The Continuity of Government concept comprises three elements:

1. Standby Officers for the Governing Body
2. Temporary Seat of Government
3. Preservation of Vital Records

An emergency or disaster could result in the injury or death of key government officials, the partial or complete destruction of established seats of government, and the destruction of public and private records essential to government operations.

Government at all levels is responsible for providing continuity of effective leadership and authority, direction of emergency operations, and management of recovery operations. To this end, the City must continue functioning as a governmental entity during and after an emergency or disaster. The California Government Code and the Constitution of California provide the authority for State and local government to reconstitute if key officials are unavailable or unable to serve.

Continuity of operations (COOP), not the subject of this EOP, consists of additional operational, logistical, and procedural elements.

9.1 RECONSTITUTION OF GOVERNMENT

California Government Code, Title 2, Division 1, Chapter 7, Article 15 ("Preservation of Local Government") establishes the primary statutory framework for continuity and reconstitution of local government in California during attack, state of emergency, or local emergency.

Article 15 contains the following provisions:

- **§8635 – Purpose:** Ensures continuity of local government during enemy attack or emergencies to preserve law and order and restore services.
- **§8636 – Definition of "Unavailable":** An officer is unavailable if killed, missing, or seriously injured; governing body decides.
- **§8637 – Succession Authority:** Political subdivisions may establish succession for department heads critical to law and safety.

- **§8638 – Standby Officers:** Governing bodies have the authority to appoint three standby officers for each member and for the chief executive.
- **§8639 – Qualifications:** Standby officers' suitability must be investigated, considering residence and work for survivability.
- **§8640 – Oath & Tenure:** Standby officers take the same oath as regular officers; serve at the pleasure of the governing body.
- **§8641 – Duties:** Standby officers must learn the role, stay informed, report for duty in emergencies, and fill posts in succession until regular officers return or replacements are chosen.
- **§8642 – Governing Body Meetings:** Must convene promptly during emergencies, even outside jurisdiction; if only one member remains, that member may reconstitute the body.
- **§8643 – Governing Responsibilities:** Assess damage, reconstitute itself and the political subdivision, and resume law and order and services.
- **§8644 – Temporary Officers:** If all governing and standby members are unavailable, temporary officers are appointed by county supervisors or nearby mayors, in order of proximity and population.

The City's municipal code (MC Chapter 2.52) establishes the primary legal framework for the City's continuity of government. The City maintains separate citywide and departmental policies and procedures that support continuity of government and continuity of operations.

9.2 DIRECTOR OF EMERGENCY SERVICES

MC § 2.52.080 designates the City Manager as the Director of Emergency Services.

Should the Director of Emergency Services be unable to serve, the Assistant City Manager(s) will automatically succeed until a permanent successor has been appointed by the City Council and seated. The Assistant City Manager(s) will have all the authority and powers of the Director of Emergency Services.

9.3 SUCCESSION OF OFFICERS

9.3.1 SUCCESSION OF CITY COUNCIL

The emergency interim succession of the City Council is permitted by California Government Code § 8638, which states:

"To provide for the continuance of the legislative and executive departments of the political subdivision during a state of war emergency or a state of emergency or a local emergency the governing body thereof shall have the power to appoint the following standby officers: (a) Three for each member of the governing body. (b) Three for the chief executive, if he is not a member of the governing body."

The City's succession list, consistent with California Government Code § 8638, is on file with the City Clerk.

9.3.2 SUCCESSION OF KEY CITY OFFICIALS

The following staff positions are key to emergency operations. The City has identified standby officers if a member is unavailable or unable to serve during a proclaimed emergency or disaster. Emergency interim lines of succession are identified in separate City policies and procedures. The succession list consistent with this section is on file with the City Clerk.

As used in this plan, the word "unavailable" means that a department head or other key City official is missing, seriously injured, deceased, or otherwise indisposed and cannot attend meetings or otherwise perform their duties. The City Manager will settle any question as to whether a particular member is unavailable.

Key positions identified as requiring emergency interim successors include:

- City Manager
- Assistant City Manager(s)
- City Attorney
- City Clerk
- Fire Chief
- Chief of Police
- Municipal Utilities & Engineering Director

- Facilities & Community Services Director
- Chief Information Officer
- Finance Director
- Human Resources Director
- Development Services Director
- Library Director
- Chief Building Official

Individuals designated as temporary successors for the above positions will immediately assume all authorities, powers, and duties of those positions when necessary.

9.4 ALTERNATE SEAT OF GOVERNMENT

The City's seats of government are provided in Table 9.4. The City also maintains virtual and remote work capabilities.

Table 9.4 City Seats of Government

CITY SEATS OF GOVERNMENT	
PRIMARY SEAT	**ALTERNATE SEAT**
City Hall 35 Cajon St, Suite 200 Redlands, CA 92373	**A.K. Smiley Public Library** 125 W Vine St Redlands, CA 92373

9.5 PRESERVATION OF VITAL RECORDS

The City is responsible for establishing measures that ensure the preservation and protection of vital records. Each department within the City will identify, maintain, and protect its vital records. Vital records are defined as those records that are essential to the rights and interests of the City, personnel, individuals, corporations and other entities, including vital statistics, land and tax records, personnel record, articles of incorporation, and historical information. Vital records also include those records essential for emergency response and recovery operations, including utility system maps, emergency supply and equipment locations, emergency operations plans and procedures, and personnel databases.

These vital records will be essential to the re-establishment of normal functions, serving to protect the rights and interests of the City. These rights and interests may include the constitution, charters, statutes, ordinances, resolutions, court records, official proceedings, and financial records of the City. The City Clerk and Deputy City Clerk, as the custodians of vital records, are responsible for maintaining, securing, and protecting all permanent records necessary for the continuity of City government.

THIS PAGE IS INTENTIONALLY LEFT BLANK

10. ADMINISTRATION, FINANCE, AND LOGISTICS

Emergency operations will be supported by the City's administrative, financial, and logistical procedures, resources, and personnel. In many cases, departments will use the same procedures and processes during emergency operations that are used during daily operations to manage similar functions. In other cases, unique emergency-specific procedures and protocols will be applied or developed to meet the needs of the emergency.

10.1 ADMINISTRATIVE PRACTICES

Adhering to established administrative and financial practices is essential for accurate resource tracking, reimbursement, and after-action reporting. City departments maintain internal procedures to support these functions, including tracking expenditures, managing resource requests, recording training, and documenting emergency exercises.

During emergencies, City departments may modify or temporarily suspend routine administrative procedures when necessary to support response and recovery operations. Such adjustments should be deliberate and guided by the City's Proclamation of Emergency, the EOC Action Plan, and the procedures outlined in this plan.

10.2 DOCUMENTATION

Timely and accurate documentation of emergency incidents is essential for conducting after-action reviews, supporting cost recovery, and legal protection. City departments are responsible for maintaining records that support these functions, including tracking expenditures, documenting recovery efforts, and preserving information for potential litigation.

When activated, the EOC Finance & Administration Section is responsible for maintaining records related to damage costs, expenditures, cost recovery, insurance claims, personnel overtime, and other emergency-related expenses. Guidance for these responsibilities is provided in the EOC Finance & Administration Section position checklists in **Part 2 (Position Checklists)** of this plan.

When activated, the Documentation Unit of the EOC Planning & Intelligence Section is responsible for collecting and maintaining all other incident records and documents.

10.2.1 AFTER-ACTION REPORTS

California Code of Regulations, Title 19, § 2450 requires any city or county declaring a local emergency for which the Governor also proclaims a State of Emergency to submit an After-Action Report to Cal OES within 90 days after the close of the incident period.

An After-Action Report serves the following important functions:

- Provides a source for documenting response and early recovery activities
- Identifies problems and successes during emergency operations
- Analyzes the effectiveness of the different SEMS components
- Identifies, documents, and facilitates corrective action for implementing and tracking improvements to existing emergency response and recovery efforts

The Fire Chief as the Emergency Manager (or designee) is responsible for coordinating the After-Action Review process and ensuring the After-Action Report is submitted.

10.3 FINANCE DURING DISASTERS

10.3.1 EMERGENCY FUNDS

Financial support for emergency response and recovery operations will generally be from funds regularly appropriated to City departments. If the demands exceed available funds, the City Manager may make additional funds available from reserve emergency funds. In that case, the City Manager has the authority under a Proclamation of Local Emergency to transfer and expend money appropriated for other purposes. Emergency expenditures will be made under the authority of the City Manager/Director of Emergency Services (MC § 2.52.100, MC § 2.52.130) unless otherwise authorized by City policy or emergency actions. Emergency finance and procurement activities will be conducted in accordance with MC § 2.16.130 and the City of Redlands Purchasing Guidelines and Procedures (February 2026).

10.3.2 DISASTER COST ACCOUNTING

Disaster-related expenditures may be eligible for reimbursement under various State and Federal programs, but the process requires thorough documentation and accurate recordkeeping to maximize recovery for eligible costs. The Finance

Department leads the City's efforts to apply for reimbursement, which can span years when infrastructure damage is extensive. Eligible costs must be directly related to the disaster response and include expenses that are reasonable, necessary, and compliant with procurement requirements. These typically cover direct costs such as salaries, equipment, materials, and contracts but exclude items like standby costs and lost revenue.

To secure funding, departments must maintain detailed records tied to original source documents from the start of the emergency. This includes payroll records, equipment logs, contractor documentation, procurement justifications, and purchase agreements. The Finance Department initiates tracking codes for emergency costs, while the EOC Finance & Administration Section compiles and submits expenditure summaries. All data must align with grant guidelines, such as those in FEMA's Public Assistance Program and Policy Guide, to ensure claims are fully supported and reimbursable.

10.4 LOGISTICS

Logistics encompasses the acquisition, tracking, and use of services, supplies, and equipment to support the EOC Action Plan and achieve emergency response and recovery objectives. The City Fire Department's Emergency Management Division leads the City's logistical preparedness and readiness activities before an emergency. City departments are responsible for planning for and having access to the emergency logistics required to carry out their assigned roles within the EOP.

When the EOC is activated, the EOC Logistics Section coordinates the acquisition, deployment, tracking, and utilization of emergency logistics to support operational priorities.

10.4.1 CITY DEPARTMENT LOGISTICS

During the preparedness phase of emergency management, City departments should take the following steps:

- Maintain current inventories of locally available resources, including equipment, personnel with specialized technical skills, supplies, and facilities
- Develop and maintain lists of out-of-area resources and mutual aid partners, including supporting agreements (e.g., MOUs, MAAs)
- Conduct just-in-time updates to all resource databases and ensure copies are transferred to the EOC in advance of or immediately prior to an emergency

- Review and test resource procurement processes, including emergency purchasing protocols and continuity of supply chains

10.4.2 EOC LOGISTICS

When activated, the EOC Logistics Section will coordinate all logistical support activities. Responsibilities include:

- Procuring, allocating, tracking, and demobilizing resources
- Coordinating personnel, facilities, equipment, supplies, and services
- Managing transportation, communications, food services, and lodging for response personnel
- Ensuring resource availability and identifying shortfalls or capability gaps

10.4.3 LOGISTICS DATABASES

Logistics and resource databases, lists, and rosters will be maintained in Digital EOC by the City Fire Department's Emergency Management Division and other City departments, including, though not limited to:

- Typed resources maintained by City departments, consistent with FEMA/NIMS resource typing standards
- Vendor and suppliers of emergency equipment and supplies
- Credentialed emergency management personnel
- Emergency facilities (e.g., shelters, staging areas, points of distribution)
- Personnel roster for deployment and staffing support
- Inventory of expendable emergency supplies (e.g., fuel, medical supplies, Personal Protective Equipment [PPE])
- Inventory of emergency sustenance supplies for EOC and field staff (e.g., food, water, hygiene items)

11. TRAINING AND EXERCISE

Training is essential for preparing public officials, emergency managers, and response personnel for disaster operations. A performance-based training program should be conducted regularly to ensure that existing staff maintain operational readiness and that new personnel gain the skills and knowledge needed to carry out their emergency responsibilities effectively.

By maintaining and adhering to a comprehensive training and exercise program, City personnel remain prepared to implement the EOP and carry out their assigned emergency responsibilities effectively.

11.1 EMERGENCY OPERATIONS TRAINING

Emergency operations training is essential to ensuring that personnel are adequately prepared to carry out their assigned emergency roles and responsibilities. The City Manager/Director of Emergency Services is ultimately responsible for ensuring the disaster readiness of City staff. City departments are responsible for scheduling and documenting the training of their respective personnel.

Personnel assigned to the City EOC should be trained for the positions they are expected to fill, consistent with the principles of SEMS and NIMS. Minimum recommended training for personnel assigned to the City's EOC are outlined below and accessible online:

- SEMS G606 (SEMS Introduction)
- IS-100 (Introduction to ICS)
- IS-200 (Basic ICS for Initial Response)
- IS-700 (An Introduction to the National Incident Management System)
- IS-800 (National Response Framework, An Introduction)
- IS-2200 (Basic Emergency Operations Center Functions)

Other position-specific training may be required for certain EOC roles, not limited to the Public Information Officer, EOC Manager, Cost Unit Leader, and Command and General Staff positions. A comprehensive and up-to-date EOC training plan is on file with, and maintained by, the Redlands Fire Department's Emergency Management Division.

The City will coordinate additional training, including training in EOC management/operations and EOC position-specific training, to ensure a trained and capable EOC Response Team. Regular refresher training is recommended for all EOC personnel, supplemented by specialized and just-in-time training based on evolving threats and operational requirements.

FEMA maintains training and credentialing frameworks under NIMS, including the National Qualification System (NQS). Cal OES provides SEMS training guidance and course standards that support local agency qualification and preparedness efforts. These may all serve as benchmarks for developing and maintaining EOC personnel qualifications. Further, the City will meet applicable training and exercise requirements tied to Federal preparedness grants.

Additional emergency operations training opportunities and courses are available from the following sources:

- Cal OES California Specialized Training Institute (CSTI)
- National Disaster & Emergency Management University through its online Independent Study Program
- Riverside Urban Area Security Initiative (UASI)

11.2 EMERGENCY OPERATIONS EXERCISES

Emergency operations exercises are essential for validating emergency operations training and providing City staff with an opportunity to carry out their assigned emergency roles and responsibilities in a safe, low-stress environment. Exercises provide a controlled environment for personnel to become proficient in emergency procedures, facilities, and systems. Local municipalities should participate in all-hazards exercises in coordination with emergency management and first response agencies, emphasizing sustained operations conducted over extended durations.

The City conducts emergency operations exercises to validate emergency plans and procedures, define section-and position-specific responsibilities, test equipment and systems, and ensure the readiness of assigned emergency personnel. City-led exercises will be conducted in accordance with SEMS, NIMS, and the Homeland Security Exercise and Evaluation Program (HSEEP), using a progressive planning approach from discussion-based to operations-based formats.

Discussion-based exercises include:

- **Seminars:** Introduce or review plans, policies, and procedures.
- **Workshops:** Build consensus, develop plans, or refine procedures.
- **Tabletop Exercises (TTX):** Explore hypothetical scenarios and test decision-making.
- **Games:** Explore decision-making and consequences in a competitive environment.

Operations-based exercises include:

- **Drills:** Test a single operation or function.
- **Functional Exercises (FE):** Test command, control, and coordination in a simulated environment.
- **Full-Scale Exercises (FSE):** Evaluate full response capabilities with deployment of personnel and equipment.

Exercises must have clearly defined objectives that relate to one or more of FEMA's Core Capabilities from the National Preparedness Goal. These capabilities span all phases of emergency management.

Exercises should include a plan for observing and assessing performance against the stated objectives. This is accomplished by exercise evaluators, who take notes, track timelines, and measure how well participants execute their roles.

After every exercise, it is important to conduct an After-Action Review and develop an After-Action Report (AAR) and Corrective Action Plan (CAP) to implement and track identified improvements. Additional information on AARs can be found in **Sections 3.17.8.1** and **10.2.1** of this plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK

12. PLAN DEVELOPMENT AND MAINTENANCE

12.1 PLAN DEVELOPMENT

The EOP was developed consistent with SEMS, NIMS, FEMA Comprehensive Preparedness Guide (CPG) 101, and the City's municipal code (MC § 2.52.150). The EOP guides the City's emergency management activities, and its development requires the input of all City departments.

EOP development has also been coordinated with the following plans:

- 2024 California State Emergency Plan (SEP)
- 2025 San Bernardino County Emergency Operations Plan (EOP)
- 2021 City of Redlands Local Hazard Mitigation Plan (LHMP)

This EOP is the principal reference source that guides the City's emergency management activities. Every City governmental function has a role in the EOP and, as such, shares the responsibility for input into its development and maintenance.

12.1.1 PLAN APPROVAL AND ADOPTION

Approval: There is no requirement for the City's emergency plan approval by any other level of government or external organization.

Adoption: Cal OES and FEMA require EOPs to be formally promulgated. To meet this requirement, the City will adopt the EOP by resolution of the City Council.

12.1.2 STANDARD OPERATING PROCEDURES BY DEPARTMENTS

City departments are expected to develop any policies, Standard Operating Procedures (SOPs), and Standard Operating Guidelines (SOGs) necessary to fulfill their roles and responsibilities under the EOP.

SOPs and SOGs may include the following:

- Guidance information
- Responsibilities of responding employees and agencies
- Policies and procedures
- Personnel assignments
- Contact lists

- Equipment lists
- Forms and documents

12.2 PLAN MAINTENANCE

The Director of Emergency Services has delegated the responsibility for developing, reviewing, and updating the EOP to the Fire Chief as the Emergency Manager (or designee). The EOP will be reviewed annually and comprehensively updated every five years.

Revisions, updates, and enhancements to the EOP that arise from routine improvement planning or corrective actions may be implemented without City Council adoption or additional legislative action.

Substantive changes to Part 1 of the EOP will be recorded in the Record of Changes table and digitally distributed to the departments listed in the Plan Distribution table. Non-substantive changes will not trigger redistribution.

Outdated versions should be destroyed following adoption of the current plan by City Council to ensure that only the most current version remains in circulation and to maintain compliance with the City's records retention policy.

CITY OF REDLANDS

35 CAJON ST, SUITE 200

REDLANDS, CA 92373

(909) 798-7555

APPENDIX A

RESOLUTION OF EOP ADOPTION

PURPOSE

This appendix includes the City Council resolution adopting the EOP.

RESOLUTION OF ADOPTION

[Insert the City Council resolution of adoption here.]

APPENDIX B

AUTHORITIES AND REFERENCES

This appendix establishes two foundations:

1. The legal basis—statutes, ordinances, executive orders, regulations, and proclamations—for emergency operations.
2. The basis for emergency authority, ensuring officials have the necessary powers to act during emergencies.

Not all authorities and references are used in the EOP Base Plan.

CITY OF REDLANDS

- City of Redlands Municipal Code, Chapter 2.52 – Emergency Organization

SAN BERNARDINO COUNTY

- County Resolution No. 229: California Master Mutual Aid Agreement. Adopted and approved on January 8, 1951.
- County Resolution No. 21.019 (b): Registered Volunteer Disaster Service Workers. County Code 21.0109 as repealed and reenacted through Ordinance No. 4191 related to volunteers. County Ordinance No. 4191 also includes additional information for registered disaster service workers entitlements under State law – under 21.0105 (b) (3).
- County Resolution No. 95-219: Adoption of Standardized Emergency Management System (SEMS). Adopted in September 1995, this Resolution contains language supporting the County's use and implementation of SEMS and the OA Concept.
- County Resolution No. 2006-329: Adoption of National Incident Management System (NIMS). Adopted NIMS and included language that the County would continue use of SEMS.
- County Resolution No. 21.0106: Establish Disaster Council. County Ordnance No. 4191 also defines the County's Disaster Council membership (21.0106) and powers/duties (21.0108).
- County Resolution No. 2022-222 Adoption of the 2022 Multi-Jurisdictional Hazard Mitigation Plan.

- County Resolution No. 2025-221, November 4, 2025, adopting the revised San Bernardino Emergency Operations Plan.
- County Code of Ordinances § 21.0103 establishing the Office of Emergency Services (2012).
- County Code of Ordinances § 21.0104 establishing the responsibilities and authorities of the Director of Emergency Services and the Manager of the Office of Emergency Services (2012).
- County Code of Ordinances § 21.0106 establishing the San Bernardino County Disaster Council.
- County Code of Ordinances § 21.0109 establishing the San Bernardino County Emergency Organization.

STATE OF CALIFORNIA

- California Assembly Bill 2311: Emergency Services - Access and Functional Needs (2016)
- California Constitution (Article XI: Local Government)
- California Coroners' Mutual Aid Plan
- California Disaster and Civil Defense Master Mutual Aid Agreement
- California Disaster Assistance Act (Title 19, Division 2, Chapter 6 of the California Code of Regulations)
- California Emergency Services Act (Title 2, Division 1, Chapter 7 of the Government Code)
- California Fire Service and Rescue Emergency Mutual Aid Plan
- California Government Code §3100, Disaster Service Workers and Public Employees
- California Law Enforcement Mutual Aid Plan
- California Senate Bill 160: Emergency Services - Cultural Competence (2019)
- California Assembly Bills 2311 and 477: Access and Functional Needs (2019)
- California Senate Bill 833: Emergencies - Office of Emergency Services - Guidelines - Alert and Warning Systems (2018)

- Disaster Service Worker Program Authorities (Title 1, Division 4, Chapter 8 of the Government Code and Section 3211.92 of the Labor Code)
- Standardized Emergency Management System (Title 19, Division 2, Chapter 1 of the California Code of Regulations)
- Standardized Emergency Management System Guidelines
- State of California Emergency Plan
- Title 19, Public Safety, Division 2, Chapter 2, Emergencies and Major Disasters, §2510
- Title 19, Public Safety, Division 2, Chapter 6, California Disaster Assistance Act, §2900

FEDERAL GOVERNMENT

- Americans with Disabilities Act of 1990 (PL 101-336) as amended
- Civil Rights Act of 1964 (PL 88-352, Section VI)
- Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans (2025)
- Federal Civil Defense Act of 1950 (PL 920)
- Homeland Security Act of 2002 (PL 107-296)
- Homeland Security Presidential Directive / HSPD-5: Management of Domestic Incidents
- Improving Access to Services for Persons with Limited English Proficiency (Executive Order 13166)
- Individuals with Disabilities in Emergency Preparedness (Executive Order 13347)
- National Incident Management System (updated 2017)
- National Response Framework (2019)
- Pets Evacuation and Transportation Standards Act of 2006 (PL 109-308)
- Post-Katrina Emergency Management Reform Act of 2006 (PL 109-295)
- Presidential Policy Directive / PPD-8: National Preparedness

- Robert T. Stafford Disaster Relief and Emergency Assistance Act (PL 93-288 as amended

APPENDIX C

ABBREVIATIONS AND ACRONYMS

Not all abbreviations and acronyms are used in the EOP Base Plan.

AAR/IP	After-Action Report/Improvement Plan
ADA	Americans with Disabilities Act
AHJ	Authority Having Jurisdiction
ARC	American Red Cross
Cal OES	California Governor's Office of Emergency Services
CALWAS	California Warning System
CALWARN	California Water/Wastewater Agency Response Network
CAP	Corrective Action Plan
CBO	Community Based Organization
CDAA	California Disaster Assistance Act
CERT	Community Emergency Response Team
CESFRS	California Emergency Services Fire Radio System
CESRS	California Emergency Services Radio System
CHP	California Highway Patrol
CISN	California Integrated Seismic Network
CLEMARS	California Law Enforcement Mutual Aid Radio System
CLERS	California Law Enforcement Radio System
CLETS	California Law Enforcement Telecommunications System
COG	Continuity of Government
CONFIRE	Consolidated Fire Agencies
COOP	Continuity of Operations
CPG	Comprehensive Preparedness Guide
CSTI	California Specialized Training Institute
CSWC	California State Warning Center

CUEA	California Utilities Emergency Association
DAFN	Disabilities or Access and Functional Needs
DENS	Dialogic Emergency Notification System
DHS	U.S. Department of Homeland Security
DOC	Department Operations Center
DSW	Disaster Service Worker
EAS	Emergency Alert System
EDIS	Emergency Digital Information Service
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EMMA	Emergency Managers Mutual Aid
EMSA	Emergency Medical Services Authority
ERNIE	Emergency Response Network of the Inland Empire
ESA	California Emergency Services Act
ESF	Emergency Support Function
FBO	Faith-Based Organizations
FCC	Federal Communications Commission
FCO	Federal Coordinating Officer
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FSE	Full-Scale Exercise
GIS	Geographic Information Systems
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
HUD	U.S. Department of Housing and Urban Development
IA	Individual Assistance

IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IDA	Initial Damage Assessment
IFGP	Individual and Family Grant Program
IPAWS	Integrated Public Alert and Warning System
ISO	California Independent Systems Operator
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
JPDA	Joint Preliminary Damage Assessment
JRIC	Joint Regional Intelligence Center (Los Angeles)
LEMA	Law Enforcement Mutual Aid
LHMP	Local Hazard Mitigation Plan
MAA	Mutual Aid Agreement
MACS	Multiagency Coordination System
MC	Municipal Code
MJHMP	Multi-Jurisdictional Hazard Mitigation Plan
MMAA	California Disaster and Civil Defense Master Mutual Aid Agreement
MOU	Memorandum of Understanding
NAWAS	National Warning System
NEIC	National Earthquake Information Center
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NQS	National Qualification System
NRF	National Response Framework

NRCS	Natural Resources Conservation Service
NVOAD	National Voluntary Organizations Active in Disaster
NWR	National Weather Radio
NWS	National Weather Service
OA	Operational Area
OASIS	Operational Area Satellite Information System
OES	Office of Emergency Services (San Bernardino County)
PA	Public Assistance
PETS	Pets Evacuation and Transportation Standards
PNP	Private Nonprofit Program
PPE	Personal Protective Equipment
PSEC	Public Safety Enterprise Communication
PSTN	Public Switched Telephone Network
RACES	Radio Amateur Civil Emergency Services
RAVE	Rave Mobile Safety (used by Redlands for emergency alerting)
RECG	Redlands Emergency Communications Group
REOC	Region Emergency Operations Center
RNA	Rapid Needs Assessment
SAP	Safety Assessment Program
SBA	U.S. Small Business Administration
SBCOVOAD	San Bernardino County Voluntary Organizations Active in Disaster
SCO	State Coordinating Officer
SEMS	Standardized Emergency Management System
SEP	California State Emergency Plan
SKYMARS	Sky Mutual Aid Radio System
SOC	State Operations Center
SOP	Standard Operating Procedure
TAP	Technical Assistance Programs

TDD/TTY	Telecommunications Device for the Deaf/Teletype
TENS	Telephone Emergency Notification System (San Bernardino County)
TTX	Tabletop Exercise
UC	Unified Command
USACE	U.S. Army Corps of Engineers
USGS	United States Geological Survey
VOAD	Voluntary Organizations Active in Disaster
WEA	Wireless Emergency Alerts
WRMAG	Western Region Mutual Assistance Group

APPENDIX D

GLOSSARY OF TERMS

Not all terms are used in the EOP Base Plan.

ACTION PLAN (AP): See EOC Action Plan and Incident Action Plan.

ACTIVATE: As used in this plan, shall mean the placing into operation of the Emergency Organization hereinafter provided for, upon the receipt of official warning of an impending or threatened emergency, or upon the declaration of the existence of a local emergency.

ADVISORY: According to the National Weather Service (NWS), an Advisory indicates that weather conditions that may cause inconvenience or minor impacts, requiring caution but typically not posing a significant threat to life or property.

AFTER-ACTION REPORT (AAR): A report that examines response actions, application of SEMS, modifications to plans and procedures, training needs and

recovery activities. After action reports are required under SEMS after any emergency that requires a declaration of an emergency. Reports must be submitted within 90 days to Cal OES.

AGENCY: A division of government with a specific function offering a particular kind of assistance. In the Incident Command System (ICS), agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance). Governmental organizations are most often in charge of an incident, though in certain circumstances private sector organizations may be included. Additionally, Non-Governmental Organizations (NGOs) may be included to provide support.

ALERT AND WARNING: Alert and warning refer to the systems and processes used by government agencies to notify partner organizations and the public of imminent threats or extraordinary hazards.

ANNEX: An addition to the EOP that provides specific information and direction. Appendix – Appendices provide relevant information already referenced in the guidance. Typically, this includes forms used or other necessary information.

APPENDIX: Appendices provide relevant information already referenced in the guidance. Typically, this includes forms used or other necessary information.

CALIFORNIA DISASTER AND CIVIL DEFENSE MASTER MUTUAL AID AGREEMENT (MMAA): An agreement entered into by and between the State of California, its various departments and agencies, and the various political subdivisions, municipal corporations, and public agencies of the State of California to assist each other by providing resources during an emergency. Mutual Aid occurs when two or more parties agree to furnish resources and facilities and to render services to each other in response to any type of disaster or emergency.

CALIFORNIA EMERGENCY FUNCTIONS (CA-EF): The California Emergency Functions are a grouping of state agencies, departments, and other stakeholders with similar functional activities/responsibilities whose responsibilities lend to improving the state's ability to collaboratively prepare for, effectively mitigate, cohesively respond to and rapidly recover from any emergency. California Emergency Functions unify a broad-spectrum of stakeholders with various capabilities, resources, and authorities to improve collaboration and coordination for a particular discipline. They also provide a framework for the state government to support regional and community stakeholder collaboration and coordination at all levels of government and across overlapping jurisdictional boundaries.

CALIFORNIA EMERGENCY SERVICES ACT (ESA): An Act within the California Government Code to ensure preparations within the state will be adequate to deal with natural, human-caused, or war-caused emergencies which result in conditions of disaster or in extreme peril to life, property, and the natural resources of the state, and generally to protect the health and safety and preserve the lives and property of the people of the state.

CATASTROPHE: As used in this plan, any natural or human-caused incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.

COMMAND: The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority.

COMMAND/MANAGEMENT: Command is responsible for the directing, ordering, and/or controlling of resources at the field response level. Management is responsible for overall emergency policy and coordination at the SEMS EOC levels.

COMMAND POST: See Incident Command Post.

COMMON OPERATING PICTURE: An overview of an incident created by collating and gathering information (e.g., traffic, weather, actual damage, resource availability, objectives, individual tasks, etc.) of any type (voice, data, etc.) from agencies and organizations in order to support decision making.

CONTINUITY OF GOVERNMENT (COG): As used in this plan, shall mean all measures taken to ensure the continuity of essential functions of government in the event of emergency conditions, including lines of succession for key decision makers and officials.

CONTINUITY OF OPERATIONS (COOP): As used in this plan, actions taken to ensure the continued performance of core capabilities and/or critical government operations during any potential incident.

CORRECTIVE ACTIONS: Implementing procedures that are based on lessons learned from actual incidents or from training and exercises.

CRISIS: Phenomenon, incident, active threat, or trend, with or without specific location, posing seemingly inevitable harm to life, property, environment, organizational performance, reputation, or way of life reasonably or ethically necessitating deliberate urgent intervention (A crisis may be local, national, or global)

CRITICAL INFRASTRUCTURE (CI): Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

CYBER THREAT: An act or threat that poses potentially devastating disruptions to critical infrastructure, including essential communications such as voice, email and internet connectivity.

CYBERSECURITY: The protection of data and systems in networks that are connected to the internet, including measures to protect critical infrastructure services. These services may include essential communications such as voice, email, and internet connectivity.

DAM FAILURE: Partial or complete collapse of a dam causing downstream flooding.

DEMOBILIZATION: The orderly, safe, and efficient return of an incident resource to its original location and status.

DEPARTMENT OPERATIONS CENTER (DOC): An Emergency Operations Center (EOC), specific to a single department or agency where the focus is on internal agency incident management and response.

DIRECTOR OF EMERGENCY SERVICES (DES): As used in this plan, shall mean the individual having jurisdiction and authority over a City's or County's response and recovery to extraordinary emergencies and disasters.

DISASTER: A sudden calamitous emergency event bringing great damage, loss, or destruction.

DISASTER SERVICE WORKER (DSW): As used in this plan, shall mean any person registered with a disaster council or the California Office of Emergency Services, or a state agency granted authority to register Disaster Service Workers, for the purpose of engaging in disaster service work pursuant to the California Emergency Services Act without pay or other consideration. Disaster Service Worker includes public employees, and also includes any unregistered persons impressed into service during a state of war emergency, a state of emergency, or a local emergency by a person having authority to command the aid of citizens in the execution of his or her duties.

EMERGENCY: As used in this plan, shall mean the actual or threatened existence of conditions of disaster or of extreme peril to the safety of persons and property within this city caused by such conditions as air pollution, fire, flood, storm, epidemic, riot, earthquake, drought, sudden and severe energy shortage, plant or animal infestation or disease, or other conditions, including conditions resulting from war or imminent threat of war, severe or imminent threat of terrorist attack, but other than conditions resulting from a labor controversy, which conditions are or are likely to require the combined services, personnel, equipment, and facilities of this city.

EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC): A congressionally ratified organization that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected state can request and receive assistance from other member states quickly and efficiently, resolving two key issues upfront: liability and reimbursement.

EMERGENCY OPERATIONS CENTER (EOC): As used in this plan, shall mean the physical location from which centralized city emergency management is performed. The physical location at which the coordination of information and

resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOC may be organized by major functional disciplines (e.g., fire, law enforcement and medical services), by jurisdiction (e.g., federal, state, tribal, city, county), or some combination thereof.

EMERGENCY OPERATIONS CENTER STAFF: Employees assigned to EOC functions to support the jurisdiction's response to an emergency event.

EMERGENCY OPERATIONS PLAN (EOP): The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

EMERGENCY RESPONSE AGENCY: Any organization responding to an emergency, or providing mutual aid support to such an organization, whether in the field, at the scene of an incident, or to an operations center.

EMERGENCY RESPONSE PERSONNEL: Personnel affiliated with or sponsored by emergency response agencies.

EOC ACTION PLAN (EAP): The plan developed at SEMS EOC levels, which contains objectives, actions to be taken, assignments, and supporting information for the next operational period.

ESSENTIAL FACILITIES: May include facilities such as law enforcement, fire, emergency operations centers, schools, medical facilities, and other resources that have a role in an effective and coordinated emergency response.

EVACUATION: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas and their reception and care in safe areas.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA): The Federal Emergency Management Agency (FEMA) is the federal agency responsible for coordinating emergency planning, preparedness, risk reduction, response, and recovery. The agency works closely with state and local governments by funding emergency programs and providing technical guidance and training. These coordinated activities at the federal, state, and local levels ensure a broad-based emergency program to ensure public safety and protect property.

FLOOD: A general and temporary condition of inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

FUNCTION: Function refers to the five major activities in ICS: Command, Operations, Planning, Logistics and Finance/Administration. The same five functions are also found at all SEMS EOC Levels. At the EOC, the term Management replaces Command. The term function is also used when describing the activity involved, (e.g., the planning function).

HAZARD: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

HAZARDOUS MATERIAL: Any substance or material that when involved in an accident and released in sufficient quantities poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

INABILITY TO ACT: As used in this plan, shall mean that an official is either killed, missing, or so seriously ill or injured as to be unable to attend meetings and otherwise perform his/her duties. Any question as to whether a particular official can be deemed to have an "inability to act" shall be settled by the governing board of the political jurisdiction or any remaining available members of said body (including standby officers who are serving on such body).

INCIDENT: An occurrence or event, natural or human-caused, which requires a response to protect life or property.

INCIDENT ACTION PLAN (IAP): An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods. At the SEMS EOC level it is called the EOC Action Plan.

INCIDENT COMMAND (IC): Responsible for overall management of the incident and consists of the Incident Commander, either single or unified command, and any assigned supporting staff. Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics, and

the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

INCIDENT COMMAND POST (ICP): The field location where the primary functions are performed. The ICP may be co-located with the incident base or other incident facilities.

INCIDENT COMMAND SYSTEM (ICS): A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

INTELLIGENCE: Product of an analytical process that evaluates information collected from diverse sources; integrates the relevant information into a cohesive package and produces a conclusion or estimate. Information must be real, accurate and verified before it becomes intelligence for planning purposes. Intelligence relates to the specific details involving the activities of an incident or EOC and current and expected conditions and how they affect the actions taken to achieve operational period objectives. Intelligence is an aspect of information. Intelligence is primarily intended for internal use and not for public dissemination.

INTEROPERABILITY: Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real-time, when needed and when authorized.

JOINT INFORMATION CENTER (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media. Public information officials from all participating agencies should co-locate at the JIC.

JOINT INFORMATION SYSTEM (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing,

recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.

JURISDICTION: A range or sphere of authority. Public agencies have jurisdiction over an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., federal, state, tribal, and local boundary lines) or functional (e.g., law enforcement, public health).

KEY RESOURCES: Any publicly or privately controlled resources essential to the minimal operations of the economy and government.

LIAISON: A form of communication for establishing and maintaining mutual understanding and cooperation.

LOCAL EMERGENCY: As used in this plan, shall mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the territorial limits of a county, city and county, or city, caused by such conditions as air pollution, fire, flood, storm, epidemic, pandemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, including conditions resulting from war or imminent threat of war, severe or imminent threat of terrorist attack, other than conditions resulting from a labor controversy, which conditions are or are likely to be beyond the control of the services, personnel, equipment, and facilities of that political subdivision and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the State Public Utilities Commission.

LOCAL GOVERNMENT: According to Federal Code 30 a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal entity, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity.

MITIGATION: Provides a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect.

MOBILIZATION: The process and procedures used by all organizations - federal, state, tribal, and local - for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.

MOBILIZATION CENTER: An off-emergency location where emergency services personnel and equipment may be temporarily located, pending assignment to emergencies, released, or reassigned.

MULTI-AGENCY OR INTER-AGENCY COORDINATION (MAC): The participation of agencies and disciplines involved at any level of the SEMS organization working together in a coordinated effort to facilitate decisions for overall emergency response activities, including the sharing of critical resources and the prioritization of incidents.

MULTI-AGENCY COORDINATION GROUP (MAC GROUP): Typically, administrators/executives, or their appointed representatives, who are authorized to commit agency resources and funds, are brought together and form MAC Groups. MAC Groups may also be known as multi-agency committees, emergency management committees, or as otherwise defined. It can provide coordinated decision-making and resource allocation among cooperating agencies and may establish the priorities among incidents, harmonize agency policies, and provide strategic guidance and direction to support incident management activities.

MULTI-AGENCY COORDINATION SYSTEM(S) (MACS): Multi-agency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The elements of multi-agency coordination systems include facilities, equipment, personnel, procedures, and communications. Two of the most commonly used elements are EOC and MAC Groups. These systems assist agencies and organizations responding to an incident.

MUTUAL AID AGREEMENTS AND/OR ASSISTANCE AGREEMENTS: Written or oral agreements between and among agencies/or organizations and/or jurisdictions

that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

MUTUAL AID COORDINATOR: An individual at the local government, operational area, region, or state level that is responsible to coordinate the process of requesting, obtaining, processing, and using mutual aid resources. Mutual Aid Coordinator duties will vary depending upon the mutual aid system.

MUTUAL AID REGION: A mutual aid region is a subdivision of Cal OES established to assist in the coordination of mutual aid and other emergency operations within a geographical area of the state, consisting of two or more operational areas.

MULTI-AGENCY OR INTER-AGENCY COORDINATION: As used in this plan, it shall mean the participation of agencies and disciplines involved at any level of the Standardized Emergency Management System (SEMS) organization working together in a coordinated effort to facilitate decisions for overall emergency response activities, including the sharing of critical resources and the prioritization of incidents.

NATIONAL: Of a nationwide character, including the federal, state, tribal and local aspects of governance and policy.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS): As used in this plan, it shall mean the adopted national emergency management processes, protocols, and procedures for federal, state, tribal and local responders. National Incident Management System (NIMS) utilizes the Incident Command System (ICS), Resource Management, Joint Information Management System, Communication and Information Management and Preparedness policies. NIMS is consistent with SEMS.

NATIONAL RESPONSE FRAMEWORK (NRF): A guide to how the nation conducts all-hazards incident management.

NATURAL DISASTER: Any hurricane, tornado, storm, flood, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, drought, fire, or other catastrophe which causes, or which may cause, substantial damage or injury to civilian property or persons**.**

NON-GOVERNMENTAL ORGANIZATION (NGO): An entity with an association based on the interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with the government. Such organizations serve a public purpose, not a private benefit. Examples of NGO include faith-based charity organizations and the American Red Cross.

OPERATIONAL AREA (OA): As used in this plan, it shall mean an intermediate level of state emergency services organization, consisting of a county and all political subdivisions within the county area. Each county geographic area is designated an operational area for the coordination of emergency activities and to serve as a link in the system of communications and coordination between the state's emergency operations centers and the operations centers of the political subdivisions comprising the operational area, as defined in California Government Code Subsection 8559 (b) and Section 8605. This definition does not change the definition of operational area as used in the existing fire and rescue mutual aid system.

OPERATIONAL AREA EMERGENCY OPERATIONS CENTER (OA EOC): The physical location at which the coordination of information and resources to support OA activities normally takes place.

OPERATIONAL PERIOD: The time scheduled for executing a given set of operation actions, as specified in the Incident Action Plan or EOC Action Plan. Operational periods can be of various lengths, although usually last 12-24 hours.

ORGANIZATION: Any association or group of persons with like objectives. Examples include, but are not limited to, governmental departments and agencies, private sector, and/or non- governmental organizations.

OUTLOOK: According to the National Weather Service (NWS), an Outlook indicates the potential for hazardous weather over the coming days, intended to provide advance awareness with low certainty and no immediate action required.

PLAN: A document that describes the broad, overall jurisdictional response to potential extraordinary emergencies or disasters.

POLITICAL SUBDIVISIONS: Includes any city, city and County, County, tax or assessment district, or other legally authorized local governmental entity with jurisdictional boundaries.

PREPAREDNESS: A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response. Within NIMS, preparedness focuses on the following elements: planning, procedures and protocols, training and exercises, personnel qualification and certification, and equipment certification.

PREVENTION: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice.

PRIVATE SECTOR: Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry.

PROTOCOLS: Sets of established guidelines for actions (which may be designated by individuals, teams, functions, or capabilities) under various specified conditions.

PUBLIC INFORMATION: Processes, procedures, and systems for communicating timely, accurate and accessible information on the incident's cause, size and current situation; resources committed; and other matters of general interest to the public, responders and additional stakeholders (both directly affected and indirectly affected).

PUBLIC INFORMATION OFFICER (PIO): A member of the Command Staff (Management Staff at the SEMS EOC Levels) responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements.

RECOVERY: The development, coordination, and execution of service and site restoration plans; the reconstitution of government operations and services; individual, private sector, non-governmental, and public assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and

economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

RECOVERY PLAN: A plan developed to restore the affected area or community.

REGION EMERGENCY OPERATIONS CENTER (REOC): Facilities found at Cal OES Administrative Regions. REOC provides centralized coordination of resources among Operational Areas within their respective regions and between the Operational Areas and the State Level.

REIMBURSEMENT: Provides a mechanism to recoup funds expended for incident-specific activities.

RESOURCE MANAGEMENT: Efficient emergency management and incident response requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under NIMS includes mutual aid agreements and assistance agreements; the use of special federal, state, tribal and local teams; and resource mobilization protocols.

RESOURCES: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.

RESPONSE: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of EOP and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

RESPONSE PERSONNEL: Includes federal, state, territorial, tribal, sub-state regional and local governments, private sector organizations, critical infrastructure owners and operators, NGO and all other organizations and individuals who assume an emergency management role. Also known as an Emergency Responder.

SITUATION REPORT: Often contains confirmed or verified information regarding the specific details relating to the incident.

SPAN OF CONTROL: The number of resources for which a supervisor is responsible, usually expressed as the ratio of supervisors to individuals. Under NIMS, an appropriate span of control is between 1:3 and 1:7, with optimal being 1:5.

SPECIAL DISTRICT: A unit of local government (other than a city, county, or city and County) with authority or responsibility to own, operate and maintain systems, programs, services, or projects (as defined in California Code of Regulations (CCR) Section 2900(s) for purposes of natural disaster assistance. This may include a joint power authority established under Section 6500 et. seq. of the Code.

STAFFORD ACT: The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) establishes the programs and processes for the federal government to provide disaster and emergency assistance to states, local governments, tribal nations, individuals, and qualified private nonprofit organizations. The provisions of the Stafford Act cover all hazards including natural disasters and terrorist events. Relevant provisions of the President. The President may declare a major disaster or emergency.

STAGING AREA: Established on an incident for the temporary location of available resources. A Staging Area can be any location on an incident in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment.

STANDARD OPERATING PROCEDURE/GUIDE (SOP/SOG): Complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS): As used in this plan shall mean the adopted State of California emergency management system. The Standardized Emergency Management System (SEMS) utilizes the Incident Command System (ICS), Multi/Interagency Coordination, Mutual Aid, and the

Operational Area Concept to facilitate emergency incident management, priority setting, interagency cooperation, and the efficient use of resources and flow of information during an emergency. SEMS is consistent with NIMS.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS) GUIDELINES: The SEMS guidelines are intended to assist those responsible for planning, implementing, and participating in SEMS.

STANDARDIZED EMERGENCY MANAGEMENT SYSTEM (SEMS) REGULATIONS: Regulations establishing the Standardized Emergency Management System (SEMS) based upon the Incident Command System (ICS) adapted from the system originally developed by the Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE) program including those currently in use by state agencies, the Multiagency Coordination System (MACS) as developed by FIRESCOPE program, the Operational Area concept and the Master Mutual Aid Agreement and related mutual aid systems. Regulations are found in TITLE 19. DIVISION 2. Chapter 1, Section 2400 et. Seq.

STATE: When capitalized, refers to any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. See Section 2 (14), Homeland Security Act of 2002, Public Law 107−296, 116 Stat. 2135 (2002).

STATEMENT: According to the National Weather Service (NWS), a Statement provides additional information, updates, or clarification about ongoing or recent weather conditions.

STATE OF EMERGENCY: As used in this plan, shall mean the duly proclaimed existence of conditions of disaster or of extreme peril to the safety of persons and property within the state caused by such conditions as air pollution, fire, flood, storm, epidemic, pandemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, other than conditions resulting from a labor controversy or conditions causing a state of war emergency, which conditions, by reason of their magnitude, are or are likely to be beyond the control of the services, personnel, equipment, and facilities of any single county, city and county, or city and require the combined forces of a mutual aid region or regions to combat, or with respect to regulated energy utilities, a sudden and

severe energy shortage requires extraordinary measures beyond the authority vested in the State Public Utilities Commission.

STATE OF WAR EMERGENCY: As used in this plan, shall mean the condition which exists immediately, with or without a proclamation thereof by the Governor, whenever this state or nation is attacked by an enemy of the United States, or upon receipt by the state of a warning from the federal government indicating that such an enemy attack is probable or imminent.

STATE OPERATIONS CENTER (SOC): The SOC is operated by the California Governor's Office of Emergency Services (Cal OES)at the State Level in SEMS. It is responsible for centralized coordination of state resources in support of the three Cal OES Administrative Regional Emergency Operations Centers (REOCs). It is also responsible for providing updated situation reports to the Governor and legislature.

SYSTEM: An integrated combination of people, equipment and processes that work in a coordinated manner to achieve a specific desired output under specific conditions.

TECHNICAL ASSISTANCE: Support provided to state, tribal and local jurisdictions when they have the resources but lack the complete knowledge and skills needed to perform the required activity (such as mobile-home park design or hazardous material assessments).

TECHNICAL SPECIALISTS: Personnel with special skills that can be used anywhere within the SEMS organization. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically certified in their fields or professions.

TERRORISM: Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any state or other subdivision of the United States in which it occurs; and is intended to intimidate or coerce the civilian population, or influence or affect the conduct of a government by mass destruction, assassination, or kidnapping.

THREAT: An indication of possible violence, harm, or danger.

TYPE: 1) An ICS resource classification that refers to capability. Type 1 is generally considered to be more capable than Types 2, 3, or 4, respectively, because of size, power, capacity, or (in the case of incident management teams) experience and qualifications. 2) A class, kind, or group sharing one or more characteristics; category. 3) A variety or style of a particular class or kind of things.

UNIFIED COMMAND (UC): An ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.

VITAL RECORDS: The essential agency records needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records), or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

VOLUNTEER: As used in this plan, a volunteer is any individual accepted to perform services by the lead agency (which has authority to accept volunteer services) when the individual performs services without promise, expectation, or receipt of compensation for services performed. A volunteer may be “affiliated” with a volunteer organization or may be “spontaneous unaffiliated” when pressed into volunteer service at the time of a disaster.

WARNING: According to the National Weather Service (NWS), a Warning indicates that a hazardous event is imminent or occurring, requiring immediate protective action.

WATCH: According to the National Weather Service (NWS), a Watch indicates that conditions are favorable for a specific hazard to develop, meaning individuals should remain alert and prepared to take action.

WebEOC: A cloud-based emergency management and continuity platform by Juvare that enables organizations to maintain a common operating picture and coordinate information, resources, and workflows during incidents and daily operations.

APPENDIX E

EOC STAFFING MATRIX

Each EOC function is assigned to one or more City department or contract agency.

EOC STAFFING MATRIX FOR CITY DEPARTMENTS	
MANAGEMENT SECTION	
POSITION	**FILLED BY**
EOC Director	City Manager's Office
EOC Coordinator	Fire Department
Liaison Officer	City Clerk's Office
Public Information Officer	Communications and Community Relations Office
Safety Officer	Human Resources Department
Security Officer	Police Department, or Call-When-Needed Contract Security Company
Legal Advisor	City Attorney
OPERATIONS SECTION	
POSITION	**FILLED BY**
Operations Section Chief	TBD – Incident Specific
Fire & Rescue Branch Director	Fire Department
Law Enforcement Branch Director	Police Department
Facilities and Community Services Branch Director	Facilities and Community Services Department
Utilities Branch Director	Municipal Utilities and Engineering Department

PLANNING & INTELLIGENCE SECTION	
POSITION	**FILLED BY**
Planning & Intelligence Section Chief	Development Services Department
Situation Analysis Unit Leader	Development Services Department (Planning Division)
Advanced Planning Unit Leader	Development Services Department
Documentation Unit Leader	Development Services Department
GIS Unit	Management Services (GIS Division)
Demobilization Unit Leader	Facilities and Community Services Department
Technical Specialists	TBD – Incident Specific
LOGISTICS SECTION	
POSITION	**FILLED BY**
Logistics Section Chief	Facilities and Community Services Department
Communications Unit Leader	Management Services (Innovation & Technology Division)
Facilities Unit Leader	Facilities and Community Services Department
Food Unit Leader	Facilities and Community Services Department
Human Resources Unit Leader	Human Resources Department
Information Technology Unit Leader	Management Services (Innovation & Technology Division)
Medical Unit Leader	Fire Department
Supply & Procurement Unit Leader	Management Services (Finance Division)
Volunteer Management Unit Leader	Human Resources Department

FINANCE & ADMINISTRATION SECTION	
POSITION	**FILLED BY**
Finance and Administration Section Chief	Management Services (Finance Division)
Compensation & Claims Unit Leader	Management Services (Finance Division)
Cost Analysis Unit Leader	Management Services (Finance Division)
Cost Recovery Unit Leader	Management Services (Finance Division)
Time Keeping Unit Leader	Management Services (Finance Division)

APPENDIX F

EMERGENCY SUPPORT FUNCTIONS CROSSWALK

The table below presents the San Bernardino County, State, and Federal Emergency Support Functions (ESF).

EMERGENCY SUPPORT FUNCTIONS		
SAN BERNARDINO COUNTY ESF	**CALIFORNIA ESF**	**FEDERAL ESF**
ESF-1 Transportation	ESF-1 Transportation	ESF-1 Transportation
ESF-2 Communications	ESF-2 Communications	ESF-2 Communications
ESF-3 Construction and Engineering	ESF-3 Construction and Engineering	ESF-3 Public Works and Engineering
ESF-4 Firefighting and Rescue	ESF-4 Fire and Rescue	ESF-4 Firefighting
ESF-5 Emergency Management	ESF-5 Management	ESF-5 Information and Planning
ESF-6 Mass Care, Sheltering, and Human Services	ESF-6 Mass Care and Shelter	ESF-6 Mass Care, Emergency Assistance, Temporary Housing, and Human Services
ESF-7 Logistics and Resource Support	ESF-7 Resources	ESF-7 Logistics
ESF-8 Public Health and Medical	ESF-8 Public Health and Medical	ESF-8 Public Health and Medical Services
ESF-9 Search and Rescue	ESF-9 Search and Rescue	ESF-9 Search and Rescue

ESF-10 Hazardous Materials	ESF-10 Hazardous Materials	ESF-10 Oil and Hazardous Materials Response
ESF-11 Food and Agriculture	ESF-11 Food and Agriculture	ESF-11 Agriculture and Natural Resources
ESF-12 Energy and Utilities	ESF-12 Utilities	ESF-12 Energy
ESF-13 Public Safety, Law Enforcement, and Security	ESF-13 Law Enforcement	ESF-13 Public Safety and Security
ESF-14 Long-Term Community Recovery	ESF-14 Recovery	ESF-14 Cross-Sector Business and Infrastructure
ESF-15 Public Information	ESF-15 Public Information	ESF-15 External Affairs
ESF-16 Evacuation and Re-Entry	ESF-16 Evacuation	
ESF-17 Volunteer and Donations Management	ESF-17 Volunteer and Donations Management	
ESF-18 Cybersecurity	ESF-18 Cybersecurity	
ESF-19 Debris Management		
ESF-20 Commodities Distribution		
ESF-21 Alert and Warning		

City Council **AGENDA ITEM NO. I11.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve the side letter agreement between the City of Redlands and Redlands Police Officers Association (RPOA), which amends and modifies Article 8 of the RPOA Memorandum of Understanding (MOU) pertaining to Field Training Officer Sergeant Incentive Pay (Human Resources/Risk Management Director King)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move to approve the side letter agreement between the City of Redlands and Redlands Police Officer Association (RPOA), which amends and modifies Article 8 of the Redlands Police Officer Association Memorandum of Understanding pertaining to the Field Training Officer Sergeant Incentive Pay.

RECOMMENDATION:

Staff recommends that the City Council approve the side letter agreement between the City of Redlands and the Redlands Police Officers Association (RPOA), which amends and modifies Article 8 of the RPOA MOU pertaining to Field Officer (FTO) Sergeant Incentive Pay.

DISCUSSION:

The proposed amendment to Article 8 of the RPOA MOU clarifies the administration of Field Training Officer (FTO) Sergeant Incentive Pay and provides the Police Department with flexibility to designate additional FTO Sergeants when operationally necessary to support the FTO program.

Following approval of this action, the Police Department’s existing internal FTO Program policy will be updated to complement the amended MOU provision. The policy will provide that when the number of participants in the field training program reaches ten (10) or more, the Chief of Police may determine that an additional Assistant FTO Sergeant is warranted. The MOU amendment further requires City Manager review and approval prior to the designation of a third Assistant FTO Sergeant.

Together, the amended MOU provision and updated department policy provide operational flexibility while establishing appropriate parameters and oversight for additional FTO Sergeant designations and the associated incentive pay.

The side letter does not modify any other wages, benefits or terms and conditions of employment contained in the current MOU. All other provisions of the existing MOU remain in full force and effect.

ALTERNATIVES:

N/A

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Gina King, Human Resources/Risk Management Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jenna Yorck, HR Manager

FISCAL IMPACT

Fiscal Year:

Revenue Generating: No

Amount:

Budgeted Y/N:

Account No.:

Additional Appropriation Required: No

Discussion:

Funding for the side letter between the City of Redlands and the Redlands Police Officer Association has been included in the FY 2027 and FY 2028 Biennial Budget.

Attachments

RPOA_Side_Letter_Sgt_FTO_10-2026v2.pdf

CITY OF REDLANDS AND THE REDLANDS POLICE OFFICERS ASSOCIATION
SIDE LETTER OF AGREEMENT (2026)

This Side Letter of Agreement amending the July 1, 2026 - June 30, 2029, Memorandum of Understanding between the Redlands Police Officers Association (RPOA) and the City of Redlands ("City") is made and entered into this 22nd day of September, 2026. RPOA and the City are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

RECITALS

WHEREAS, on June 16, 2026, RPOA and the City agreed to a Memorandum of Understanding ("RPOA MOU") for the period of July 1, 2026 to June 30, 2029; and

WHEREAS, the Parties now wish to clarify their intentions with respect to Article 8 of the RPOA MOU; and

WHEREAS, representatives of the City and RPOA have met and conferred in good faith and now wish to effect changes with respect to Article 8 of the RPOA MOU.

NOW, THEREFORE, in consideration of the mutual promises contained herein, RPOA and the City agree as follows:

AGREEMENT

Article 8 of the RPOA MOU, entitled " Field Training Officer Sergeant Incentive Pay" is hereby amended to read as follows:

Effective the first full pay period after July 1, 2026, or the first full pay period after City Council approval of this MOU, whichever is later, the Sergeant overseeing the Field Training Officer (FTO) program shall receive FTO pay in the amount of five percent (5%) of (Base Salary + Longevity Pay + POST Certification Pay). This pay differential shall only be paid while the employee is serving as the FTO Sergeant.

The Chief of Police, at their sole discretion, may designate additional Sergeants to assist with the administration of the FTO program however, prior to designating a third Assistant FTO Sergeant, the Chief of Police shall submit a request and obtain approval by the City Manager. This pay differential shall only be paid when the employee has been designated by the Chief of Police as an Assistant FTO Sergeant and while the employee is supporting the FTO program.

All other provisions in this article remain unchanged.

CITY OF REDLANDS	REDLANDS POLICE OFFICER ASSOCIATION
Mario Saucedo, Mayor	Jeffrey Frisch, President

Attest:

Jeanne Donalson, City Clerk

City Council **AGENDA ITEM NO. I12.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve a Fourth Amendment to the Professional Services Agreement with Carollo Engineers, Inc. for the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project extending the completion time to December 31, 2028 (Municipal Utilities and Engineering Director Heredia)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move that the City Council approve the Fourth Amendment to the Professional Services Agreement with Carollo Engineers, Inc. for the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project, extending the completion date to December 31, 2028.

RECOMMENDATION:

Staff recommends that the City Council approve of the Fourth Amendment to the Professional Services Agreement with Carollo Engineers, Inc. for the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project, extending the completion date to December 31, 2028.

DISCUSSION:

The City extracts groundwater and receives raw water from two (2) surface water sources for treatment and disinfection to meet drinking water standards prior to distribution through the potable water system. Santa Ana River surface water is received and treated at the Hinckley Water Treatment Plant, and Mill Creek surface water is received and treated at the Tate Water Treatment Plant (Tate). Tate has a potable water treatment capacity of twenty million gallons per day (20 MGD), with average daily production of seven (7) MGD and peak day production of eleven (11) MGD during the peak water use season (July-September). Tate operates in the 2,340' pressure zone and is able to supply approximately eighty-seven percent (87%) of the City's water service area customers. The Tate facility has been upgraded, and its processes enhanced to improve water supply reliability by allowing State Water Project water to be mixed with Mill Creek water for treatment. Brady & Associates, Inc. recently completed a Condition, Structural, and Seismic Assessment of the Tate raw water transmission pipeline and recommended replacement.

The goal of this phase of the Tate WTP Raw Water Influent Pipeline Replacement Project (Project) is to engineer a new raw water influent pipeline from the box structure near the Southern California Edison Power House #1, across Mill Creek, and connect to existing pipeline valving at the Tate connection point. The Project also serves as a distribution for Crafton Water Company and the San Bernardino Valley Water Conservation District, and includes valves and flow meters to separately control and measure flows. The Project will likely be constructed in two (2) separate phases in the future, and construction documents will be provided for each phase.

On April 19, 2022, the City Council approved a Professional Services Agreement with Carollo Engineers, Inc. (Carollo), for this phase of the Project and determined the Project to be exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act. On October 3, 2023, the City Council approved the First Amendment to the Agreement, extending the completion term by twelve (12) months to October 18, 2024. On October 1, 2024, the City Council approved the Second Amendment to the Agreement, extending the completion term by an additional twelve (12) months to October 18, 2025. On September 2, 2025, City Council approved the Third Amendment to the Agreement, extending the completion term by an additional twelve (12) months to October 18, 2026.

Continued delays in coordinating engineering reviews and obtaining the necessary permits from external agencies necessitate an additional extension of the contract term. Upon completion of the final design, the Project will require final review and permitting by the applicable agencies, a process that may take several months to a year to complete. The consultant will also provide necessary support during the bidding process to assist the City with solicitation, bid evaluation, and award of the construction contract. If the Fourth Amendment is approved, the amended completion date will be December 31, 2028. No additional revisions to the Agreement are proposed.

ALTERNATIVES:

The City Council may choose not to approve the Fourth Amendment and provide alternative direction to staff.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Monica Heredia, Municipal Utilities and Engineering Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Goutam Dobey, City Engineer

FISCAL IMPACT

Fiscal Year: FY 26/27

Account No.: N/A

Amount:

Budgeted Y/N:

Account No.:

Additional Appropriation Required:

Discussion:

There is no fiscal impact associated with this action.

Attachments

A_Fourth_Amendment_-_Carollo_Engineers.pdf
B_Agreement_-_Carollo_Engineers_Reference.pdf
C_First_Amendment_-_Carollo_Engineers_Reference.pdf
D_Second_Amendment_-_Carollo_Engineers_Reference.pdf
E_Third_Amendment_-_Carollo_Engineers_Reference.pdf

FOURTH AMENDMENT TO AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This fourth amendment ("Fourth Amendment") to the agreement for Engineering services related to the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project dated April 19, 2022 ("Agreement"), by and between the City of Redlands, a municipal corporation ("City"), and Carollo Engineers, Inc., a Delaware corporation ("Consultant") is made and entered into this 6th day of October, 2026.

RECITALS

WHEREAS, it is the desire of the City and Consultant to amend their existing Agreement, specifically to extend the contract term to December 31, 2028, and make other minor changes.

NOW, THEREFORE, for good and valuable consideration in the receipt of which is hereby acknowledged, City and Consultant agree as follows:

AGREEMENT

Section 1. Article 3 ("Responsibilities of City") Section 3.1 is hereby amended to read as follows:

"3.1 City designates Monica Heredia, Municipal Utilities and Engineering Department Director, as City's representative with respect to performance of the Services, and such person shall have the authority to transmit instructions, receive information, interpret and define City's policies and decisions with respect to performance of the Services."

Section 2. Article 4 ("Performance of Services") Section 4.2 is hereby amended to read as follows:

"4.2 Consultant shall complete the Services by December 31, 2028, unless the Services are terminated earlier as provided for herein."

Section 3. All other provisions of the Agreement shall remain unchanged by this Fourth Amendment and in effect.

IN WITNESS WHEREOF, the parties have executed this Fourth Amendment, to be effective as of October 6, 2026.

CITY OF REDLANDS

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

CAROLLO ENGINEERS, INC.

By: _____
Graham J.G. Juby, Senior Project Manager

AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This agreement for the provision of professional engineering services ("Agreement") is made and entered in this 19th day of April, 2022 ("Effective Date"), by and between the City of Redlands, a municipal corporation and general law city ("City") and Carollo Engineers, Inc., a Delaware corporation ("Consultant"). City and Consultant are sometimes individually referred to herein as a "Party" and, together, as the "Parties." In consideration of the mutual promises contained herein, City and Consultant agree as follows:

ARTICLE 1 – ENGAGEMENT OF CONSULTANT

1.1 City hereby engages Consultant to design and prepare plans and specifications for City for a replacement raw influent pipeline and associated facilities to supply the Tate Water Treatment Plant to be constructed in the future (the "Services").

1.2 The Services shall be performed by Consultant in a professional manner, and Consultant represents that it has the skill and the professional expertise necessary to provide the Services to City at a level of competency presently maintained by other practicing professional consultants in the industry providing like and similar types of Services.

ARTICLE 2 – SERVICES OF CONSULTANT

2.1 The Services that Consultant shall perform are more particularly described in Exhibit "A," titled "Scope of Services," which is attached hereto and incorporated herein by reference.

2.2 Consultant shall comply with applicable federal, state and local laws and regulations in the performance of this Agreement including, but not limited to, any applicable State prevailing wage laws.

2.3 Consultant shall not be liable to and/or indemnify City and/or any third party related to any inconsistencies between Consultant's data projections and estimates and actual costs and/or quantities realized by City and/or any third party in the future, except to the extent such inaccuracies are caused by Consultant's negligent performance hereunder.

ARTICLE 3 – RESPONSIBILITIES OF CITY

3.1 City designates John R. Harris, Municipal Utilities and Engineering Department Director, as City's representative with respect to performance of the Services, and such person shall have the authority to transmit instructions, receive information, interpret and define City's policies and decisions with respect to performance of the Services.

3.2 City shall furnish Consultant available studies, reports and other data pertinent to Consultant's services; obtain or authorize Consultant to obtain or provide additional reports and data as required; furnish to Consultant services of others required for the performance of Consultant's services hereunder, and Consultant shall be entitled to use

and reasonably rely upon all such information and services provided by City or others in performing Consultant's services under this Agreement.

3.3 Documents, including drawings and specifications, prepared by Consultant pursuant to this Agreement are not intended or represented to be suitable for reuse by City or others for this project or on any other project. Any reuse of completed documents or use of partially completed documents without written verification or concurrence by Consultant for the specific purpose intended will be at City's sole risk and without liability or legal exposure to Consultant.

3.4 City shall arrange for access to and make all provisions for Consultant to enter upon public and private property as required for Consultant to perform services hereunder.

ARTICLE 4 – PERFORMANCE OF SERVICES

4.1 Consultant shall perform and complete the Services in a prompt and diligent manner in accordance with the schedule set forth in Exhibit "A," titled "Consultant Proposal," which is attached hereto and incorporated herein by reference.

4.2 The term of this Agreement shall be for a period of eighteen (18) months from the Effective Date of this Agreement, unless terminated earlier as provided herein.

4.3 If Consultant's Services include deliverable electronic visual presentation materials, such materials shall be delivered in a form, and made available to City, consistent with City Council-adopted policy for the same. It shall be the obligation of Consultant to obtain a copy of such policy from City staff.

4.4 Consultant is not responsible for damage or delay in performance caused by events beyond the reasonable control of Consultant. In the event Consultant's services are suspended, delayed or interrupted for the convenience of City or delays occur beyond the reasonable control of Consultant, an equitable adjustment in Consultant's time of performance and cost of Consultant's personnel and subcontractors may be made.

ARTICLE 5 – PAYMENTS TO CONSULTANT

5.1 Total compensation for Consultant's performance of the Services shall not exceed the amount of eight hundred thirty five thousand five hundred forty nine dollars ($835,549). City shall pay Consultant on a time and materials basis up to the not to exceed amount in accordance with Exhibit "B," titled "Cost Proposal," which is attached hereto and incorporated herein by reference.

5.2 Consultant shall submit monthly invoices to City describing the Services performed during the preceding month. Consultant's invoices shall include a brief description of the Services performed, the dates the Services were performed, the number of hours spent and by whom, and a description of reimbursable expenses related to the Services. City

shall pay Consultant no later than thirty (30) days after receipt and approval by City of Consultant's invoice.

5.3 Any notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a Party may provide notice in accordance with this section:

CITY:	CONSULTANT:
John R. Harris, MUED Director	Graham J.G. Juby, Senior Project Manager
City of Redlands	Carollo Engineers, Inc.
35 Cajon Street, Suite 15A	3400 Central Avenue, Suite 205
P.O. Box 3005 (mailing)	Riverside, CA 92506
Redlands, CA 92373	GJGJuby@carollo.com
jharris@cityofredlands.org	Phone: (951) 776-3955
Phone: (909) 798-7658	Fax: (951) 776-4207

ARTICLE 6 – INSURANCE AND INDEMNIFICATION

6.1 The following insurance coverage required by this Agreement shall be maintained by Consultant for the duration of its performance of the Services. Consultant shall not perform any Services unless and until the required insurance listed below is obtained by Consultant. Consultant shall provide City with certificates of insurance and endorsements evidencing such insurance prior to commencement of the Services. Insurance policies shall include a provision prohibiting cancellation or modification of the policy except upon thirty (30) days prior written notice to City.

A. Workers' Compensation and Employer's Liability insurance in the amount that meets statutory requirements with an insurance carrier acceptable to City, or certification to City that Consultant is self-insured or exempt from the workers' compensation laws of the State of California. Consultant shall execute and provide City with Exhibit "C," titled "Workers' Compensation Insurance Certification," which is attached hereto and incorporated herein by this reference, prior to performance of the Services.

B. Comprehensive General Liability insurance with carriers acceptable to City in the minimum amount of One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) aggregate, for public liability, property damage and personal injury is required. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

C. Consultant shall secure and maintain professional liability insurance throughout the term of this Agreement in the amount of One Million Dollars ($1,000,000) per claim made.

D. Business Auto Liability coverage, with minimum limits of One Million Dollars ($1,000,000) per occurrence, combined single limit bodily injury liability and property damage liability. This coverage shall include all Consultant owned vehicles used in connection with Consultant's provision of the Services, hired and non-owned vehicles, and employee non-ownership vehicles. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

E. Consultant is expressly prohibited from assigning or subcontracting any of the Services without the prior written consent of City. In the event of mutual agreement by the Parties to assign or subcontract a portion of the Services, Consultant shall add such assignee or subcontractor as an additional insured to the insurance policies required hereby and provide City with the insurance endorsements prior to any Services being performed by the assignee or subcontractor.

6.2 Consultant shall defend, indemnify and hold harmless City and its elected and appointed officials, employees and agents from and against any and all claims, losses or liability, including attorneys' fees, arising from injury or death to persons or damage to property to the extent caused by any negligent act or omission by, or the willful misconduct of, Consultant, or its officers, employees and agents in performing the Services. In no event shall the cost to defend charged to Consultant exceed Consultant's proportionate percentage of fault.

6.3 Neither party shall be responsible for economic, incidental and/or consequential damages to the other party and/or any third party. Additionally, Consultant shall not be responsible for acts and decisions of third parties, including governmental agencies, other than Consultant's subconsultants, that impact project completion and/or success. Consultant and its subconsultants shall only be liable for any damage caused by negligence related to cleaning activities required to facilitate the CCTV inspection.

ARTICLE 7 – CONFLICTS OF INTEREST

7.1 Consultant covenants and represents that it does not have any investment or interest in any real property that may be the subject of this Agreement or any other source of income, interest in real property or investment that would be affected in any manner or degree by the performance of Consultant's Services. Consultant further covenants and represents that in the performance of its duties hereunder, no person having any such interest shall perform any Services under this Agreement.

7.2 Consultant agrees it is not a designated employee within the meaning of the Political Reform Act because Consultant:

A. Does not make a governmental decision whether to:

(i) approve a rate, rule or regulation, or adopt or enforce a City law;
(ii) issue, deny, suspend or revoke any City permit, license, application, certification, approval, order or similar authorization or entitlement;
(iii) authorize City to enter into, modify or renew a contract;
(iv) grant City approval to a contract that requires City approval and to which City is a party, or to the specifications for such a contract;
(v) grant City approval to a plan, design, report, study or similar item;
(vi) adopt, or grant City approval of, policies, standards or guidelines for City or for any subdivision thereof.

B. Does not serve in a staff capacity with City and in that capacity, participate in making a governmental decision or otherwise perform the same or substantially the same duties for City that would otherwise be performed by an individual holding a position specified in City's Conflict of Interest Code under Government Code section 87302.

7.3 In the event City determines that Consultant must disclose its financial interests, Consultant shall complete and file a Fair Political Practices Commission Form 700, Statement of Economic Interests, with the City Clerk's office pursuant to the written instructions provided by the City Clerk.

ARTICLE 8 – GENERAL CONSIDERATIONS

8.1 In the event any action is commenced to enforce or interpret any of the terms or conditions of this Agreement the prevailing Party shall, in addition to any costs and other relief, be entitled to the recovery of its reasonable attorneys' fees, including fees for the use of in-house counsel by a Party.

8.2 Consultant shall not assign any of the Services, except with the prior written approval of City and in strict compliance with the terms and conditions of this Agreement. Any assignment or attempted assignment without such prior written consent may, in the sole discretion of City, result in City's immediate termination of this Agreement.

8.3 Consultant is for all purposes under this Agreement an independent contractor and shall perform the Services as an independent contractor. Neither City nor any its agents shall have control over the conduct of Consultant or Consultant's employees, except as herein set forth. Consultant shall supply all necessary tools and instrumentalities required to perform the Services. Assigned personnel employed by Consultant are for its account only, and in no event shall Consultant or personnel retained by it be deemed to have been employed by City or engaged by City for the account of, or on behalf of City. Consultant shall have no authority, express or implied, to act on behalf of City in any capacity whatsoever as an agent, nor shall Consultant have any authority, express or implied, to bind City to any obligation.

8.4 This Agreement may be terminated by City, in its sole discretion, by providing not less than five (5) days prior written notice to Consultant of City's intent to terminate. If this Agreement is terminated by City, an adjustment to Consultant's compensation shall be made, but (1) no amount shall be allowed for anticipated profit or unperformed Services, and (2) any payment due Consultant at the time of termination may be adjusted to the extent of any additional costs to City occasioned by any default by Consultant. Upon receipt of a termination notice, Consultant shall immediately discontinue its provision of the Services and, within five (5) days of the date of the termination notice, deliver or otherwise make available to City, copies (in both hard copy and electronic form, where applicable) of project related data, design calculations, drawings, specifications, reports, estimates, summaries and such other information and materials as may have been accumulated by Consultant in performing the Services. Consultant shall be compensated on a pro-rata basis for Services completed up to the date of termination.

8.5 Consultant shall maintain books, ledgers, invoices, accounts and other records and documents evidencing costs and expenses related to the Services for a period of three (3) years, or for any longer period required by law, from the date of final payment to Consultant pursuant to this Agreement. Such books shall be available at reasonable times for examination by City at the office of Consultant.

8.6 This Agreement, including the Exhibits incorporated herein by reference, represents the entire agreement and understanding between the Parties as to the matters contained herein, and any prior negotiations, written proposals or verbal agreements relating to such matters are superseded by this Agreement. Except as otherwise provided for herein, any amendment to this Agreement shall be in writing, approved by City and signed by City and Consultant.

8.7 This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions. The Parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated only in the state courts located in San Bernardino County, California, and the federal courts located in Riverside County, California.

8.8 If one or more of the sentences, clauses, paragraphs or sections contained in this Agreement is declared invalid, void or unenforceable by a court of competent jurisdiction, the same shall be deemed severable from the remainder of this Agreement and shall not affect, impair or invalidate the remaining sentences, clauses, paragraphs or sections contained herein, unless to do so would deprive a Party of a material benefit of its bargain under this Agreement.

8.9 The services to be performed by Consultant are intended solely for the benefit of City. No person or entity not a signatory to this Agreement shall be entitled to rely on Consultant's performance of its services hereunder, and no right to assert a claim against Consultant by assignment of indemnity rights or otherwise shall accrue to a third party as a result of this Agreement or the performance of Consultant's services hereunder.

IN WITNESS WHEREOF, duly authorized representatives of City and Consultant have signed in confirmation of this Agreement.

CITY OF REDLANDS

By: _____
Paul T. Barich, Mayor

CAROLLO ENGINEERS, INC.

By: _____
Graham J.G. Juby, Senior Project Manager

ATTEST:

_____
Jeanne Donaldson, City Clerk

By: _____
Eric M. Mills, Client Services Director

EXHIBIT "A"

SCOPE OF SERVICES

[ATTACHED]

CITY OF REDLANDS
MUNICIPAL UTILITIES & ENGINEERING DEPARTMENT

TATE WTP RAW WATER INFLUENT LINE REPLACEMENT PROJECT

CAROLLO ENGINEERS

SCOPE OF WORK

The Tate Water Treatment Plant (WTP) has a potable water treatment design capacity of twenty (20) million gallons per day (MGD), with average daily production of seven (7) MGD and peak day production of eleven (11) MGD during the peak water use season (July – August). This WTP operates in the 2,340' pressure zone. The City has added enhancements to the Tate WTP that provide more water supply reliability by allowing State Water Project water to mixed with Mill Creek water for treatment. Brady & Associates, Inc. (Brady) recently completed a condition, structural, and seismic assessment of the Tate WTP raw water transmission line and recommended a new parallel pipeline to be constructed.

The purpose of this project is to engineer and construct a new influent pipeline from the box structure near Power House No. 1, across Mill Creek Channel and connecting to the Tate WTP connection point identified in the RFP. This project also includes a distribution line to Crafton Water Company with two separate valve and flow meter vaults. The influent pipeline will be constructed in two phases per RFP, Addendum No. 1 requirements. For this reason, we have estimated two separate sets of construction documents (plans, specifications, and cost estimates) will be prepared as part of the final design.

The scope of work detailed below is intended to capture all tasks necessary to allow for preparation of bidding and construction documents for the proposed project. Several optional tasks have also been included for the City to consider.

Task 1 – Project Management and Meetings

It is assumed that the project will take approximately 14-months to complete. This task includes general project management and meetings.

A. Prepare monthly invoices including a Progress Report summarizing work performed for the invoice period, supporting tabulation of hours by date and task for employees working on the project, and supporting expense reports and invoices for reimbursable expenses.
B. Attend monthly 90-minute project meetings with the MUED staff to discuss project progress and any engineering issues that arise. Meetings may be performed remotely. Meeting agendas will be established in collaboration with MUED staff. A total of 8 project meetings has been assumed.

C. Attend six in-person 90-minute design review meetings. In place of a monthly project meeting, attend in-person design review meetings as follows:
    a. Project kickoff meeting,
    b. Pipeline Alternatives meeting,
    c. 30% design review meeting,
    d. 60% design review meeting,
    e. 90% design review meeting,
    f. Final design completion meeting.

Carollo will develop a data needs list that will be submitted to City before or at the kickoff meeting. The list will be updated as the project proceeds identifying data received and data still to be received. Data received from City will be reviewed as needed to provide information for the project.

Meeting agendas will be established in collaboration with MUED staff.

Deliverables: Meeting Agendas, Meeting Notes, Presentation Materials, Monthly Invoices, Monthly Progress Reports, Date Needs List in electronic format. List will be updated regularly as needed.

Task 2 – Pipeline Alternatives Evaluation

Carollo will review the Brady assessment and recommendations and conduct additional research and site investigations necessary to evaluate up to three separate pipeline alignments and the construction alternatives listed below to replace the Tate WTP raw water transmission line, including associated valves, control and metering systems (including SCADA), and plumbing systems. It has been assumed that no additional assessment of the existing transmission line is necessary. An important component of this project is the addition of equipment necessary to connect to, and meter, water delivered to Crafton Water Company and to the San Bernardino Valley Water Conservation District. Carollo will evaluate up to three pipeline alternatives, including both trenched and trenchless construction alternatives. Carollo will provide a list of pros and cons for various replacement construction alternatives, including:

1. Construction of a replacement transmission line with the same diameter or larger, and along the same alignment;

2. Construction of a replacement transmission line with the same diameters evaluated for Alternative 1, along a modified alignment to the west of the existing line;

3. Construction of a replacement transmission line with the same diameters considered for Alternatives 1 and 2, along a modified alignment to the east of the existing line.

4. Rehabilitation of the existing transmission line, and construction of a redundant transmission line (side-by-side and along a new alignment).

A. Carollo will provide conceptual land acquisition (if necessary) and construction cost estimates, including site civil work, access roads, fencing, piping, and control systems, and other associated temporary and permanent construction elements for each of the replacement construction alternatives. At the conclusion of Task 2, the City staff will select a preferred construction alternative and alignment. Carollo will prepare Technical Memorandum (TM) No. 1 that will be the basis for selection of the preferred alternative and which will consider the following minimum items:

   a. **Condition Assessment/Rehabilitation.** Review the Brady condition assessment report. It has been assumed that additional interior, or exterior condition assessment work will not be required. Should such additional work be determined as being needed in order to complete the design, then this will be discussed separately with the City and a suitable approach identified.

   b. **Material Types.** Evaluate various construction material types to rehabilitate and/or replace the raw water transmission line.

   c. **Hydraulics.** Evaluate the hydraulic implications of various pipe configurations (e.g., single line, redundant line, control systems, pumping needs, piping schematics, etc.).

   d. **Water Quality.** Identify implications of water quality on various pipe configurations and material types.

   e. **Foundations.** At a planning level, identify typical pipe support foundation alternatives, casing pipe needs, and identify any slope-stability concerns, all as appropriate.

   f. **Regulatory Constraints.** Research and identify any regulatory constraints (e.g., SWRCB, USACE, DDW, Air Quality Management Division, Caltrans etc.) that may have implications on the foundation and/or pipe location, material type, or geometry. Research and identify necessary construction permitting and the level of CEQA evaluation and documentation necessary for each alternative. Prepare a table and schedule to indicate the anticipated permit requirements and timeline anticipated for obtaining each permit.

B. Evaluate life cycle costs (as net present and annual worth) for alternatives under consideration. This shall include the initial capital investment as well as anticipated maintenance and replacement costs.

C. Present results of the alternatives evaluation to MUED staff for selection of the preferred alternative. The alternative evaluation will be presented as part of TM-1. Figures, photographs, and estimate tables accompanied by a meeting/presentation materials will be included as an Appendix to TM-1.

After receiving the City's comments on the draft TM-1, Carollo will prepare and submit a final version of TM-1 which will be used as the basis for the design phase.

Deliverables: Draft and Final versions of TM-1 and supporting exhibits in electronic format.

Task 3 - Site Survey and Basemap Preparation

Carollo will sub-contract with a surveyor to conduct the following work:

A. Perform a site survey within the project area for existing surface features, topography, and utilities as necessary for engineering. Utility data shall be obtained by performing 811 utility locates and will likely require follow up with individual utility companies who fail to locate their lines. City will provide existing shapefiles for water, sewer, and storm utilities to supplement field surveys.
B. Perform field surveys as necessary to establish property boundaries and easements adjoining the project site.
C. Perform the potholing of existing utilities where necessary to collect data for design (e.g., elevations at critical crossings or where potential for conflict exists). Survey the locations of exposed utilities.
D. Coordinate jet-tracing of any gravity utility lines that require tracing and survey the marked locations. The actual jet-tracing will be performed by the City.
E. Establish local survey control within the project area and place survey control monuments as necessary along the project alignment. Monuments shall be a #5 set rebar at least four feet (4') deep with an aluminum cap.
F. Prepare an AutoCAD basemap of the project for use in subsequent planning, design, and plan preparation.

Deliverables: AutoCAD basemap of the site for use in subsequent planning, design, and plan preparation.

Task 4 - Geotechnical Investigations

Carollo will sub-contract with a geotechnical consultant to conduct the following work:

A. Perform geotechnical borings and laboratory analyses as necessary to engineer the proposed pipe foundations and site improvements.
B. Perform soil analyses to determine the corrosion potential along the pipeline alignment and develop a cathodic protection system as necessary based on the analyses results.
C. Perform slope-stability studies as necessary to aid in final siting of the pipe and foundations, and identify any special considerations required to maintain stability of the areas and avoid compromising the pipe and foundations or associated improvements.
D. Prepare a geotechnical report summarizing the methods, findings, and recommendations resulting from the geotechnical investigations.

Deliverables: Draft and Final versions of a Geotechnical Report in electronic format.

Task 5 - Final Engineering

A. Carollo will perform the final engineering of the preferred alternative to include the raw water transmission line, foundations, control structures, instrumentation, manholes and vaults, and any other elements necessary to bring the system into service. Final engineering will include provisions for connections to existing Tate WTP system piping.

B. Engineer site improvements within the project areas to include site grading, drainage, perimeter fencing, and access roadways. Given the small scale of the project (less than 1 acre of additional impervious area created), it is anticipated that stormwater detention and permanent water quality BMPs are not required.

C. Coordinate with dry utility companies (gas, power, communications, etc.) to relocate any existing utilities in conflict with the proposed improvements. The actual relocation designs will be performed by the utility owners and billed to City.

D. Coordinate Engineering with outside agencies based on the findings in TM-01 (i.e., San Bernardino County Flood Control District, USACE, RWQCB, FEMA, etc.) to include permitting, design reviews, specification reviews, etc. Actual permitting fees will be paid by City.

E. Engineer erosion control plans indicating erosion control minimums to be implemented by the Contractors. A detailed SWPPP is outside of the scope of work and will be prepared by the Contractors.

Construction Documents

A. Prepare suitable-for-construction engineering drawings for the project to include, but not be limited to, the following:
    a. Title Sheet
    b. General Notes Sheet
    c. Existing Conditions Sheet (with identification of available project access and staging areas)
    d. Survey Control Sheet
    e. Erosion Control Plan
    f. Removal/Demolition Plans
    g. Pipe Plans (including foundations, piping, plans and profiles)
    h. Connection Piping Details
    i. Control System Plans
    j. Utility/Power Plans (as necessary)
    k. Utility Relocation Plans
    l. Site Grading and Drainage Plans
    m. Site Security Plans (perimeter fencing and access gates)
    n. Detail Sheets (as necessary)
    o. Site Restoration Plans

p. Additional plan sheets necessary to create a plan set suitable for bidding and construction

B. Prepare detailed specifications for project construction.

C. Plans and specifications shall be submitted to the City for review and comment at the 30%, 60%, 90%, and final design completion level.

D. Using a bid form prepared in collaboration with City, prepare a summary of quantities for the final design.

E. Prepare an engineer's opinion of probable construction cost at the 30%, 60%, 90%, and final design completion levels.

Task 5.1 – 30% Design

A preliminary drawing list that includes the anticipated 100% submittal drawing list is included in Attachment A. This attachment includes a separate preliminary list of drawings for Phase 1 and Phase 2. This list of drawings may be adjusted based on the findings of Task 2 described above. The drawings will be prepared in the current Carollo version of Bentley's Microstation or Revit and converted to AutoCAD files, and the specifications will be prepared in the current Carollo version of Microsoft Word in the 17-Division format. Project will use the City Front-End Specifications (Division 0), which will be provided by the City. Division 1 and the other technical specifications will be provided by Carollo.

The 30% submittal drawings will include sufficient early development to display the basic format of the plan set for each of the disciplines required to complete the work. The submittal will include the basic organization sheets, sufficient detail to show the basic layout of facilities, process instrumentation and control diagrams, SCADA Block Diagram, and single line power diagrams, as needed. The plans will provide specific horizontal and vertical control for all proposed underground facilities.

The specifications will include a summary Table of Contents for all specifications anticipated for the project. Specifications included at this point will still include marked-up sections, for further development.

After review of the 30% submittal by City, a design review meeting will be held with City to review and discuss their comments. The City's comments on the 30% drawings will be incorporated into the 60% design submittal.

Preliminary Construction Cost Estimate - A preliminary construction cost estimate will be prepared and included as part of the 30% Submittal. A separate construction cost estimate will be provided for Phase 1 and Phase 2.

Deliverables: 30% Design Package that includes selected drawings to approximately 30% level of completion for Phases 1 and 2 and Technical Specifications Table of Contents, and opinion of probable construction cost, all as a pdf set of the drawings and specifications files.

Task 6.2 – Final Design

Following receipt of the City's comments on the 30% Design Submittal, Carollo will advance the design to approximately 60%. Provide a 60% Design Submittal to the City that now includes all drawing sheets anticipated in the two Bid Sets, and all specifications, although some may still need to be finalized. With the 60% submittal include an updated construction cost estimate for both Phases of the project.

After the City's review period, Carollo will meet with City to receive comments and feedback on the plans and specifications in a design review meeting.

Following receipt of the City's comments on the 60% Design Submittal, Carollo will advance the design to 90%. Carollo will provide a 90% Design Submittal to the City that now includes a complete set of drawing sheets and all specifications separated into Phase 1 and Phase 2 packages. In parallel with the City's review of the 90% submittal, conduct an in-house QA/QC check of the plans and specifications.

After the City's review period, Carollo will meet with City to receive comments and feedback on the plans and specifications.

Following receipt of the City's comments on the 90% Design Submittal, and comments from Carollo's in-house checking team, Carollo will advance the design to 100% incorporating all comments. Carollo will provide a 100% Design Submittal to the City that now includes a complete set of all drawing sheets and all specifications for both Phase 1 and Phase 2 packages. Together with 100% submittal, submit the final Engineer's Opinion of Probable Construction Cost.

Using a bid form prepared in collaboration with City, Carollo will prepare a summary of quantities for the final design and submit those with the 100% Submittal.

Carollo will incorporate any final comments into the documents and prepare and submit the two Bid Set packages for Phase 1 and Phase 2.

Deliverables: 60%, 90% and 100% Design Drawings and Specifications all in PDF format. Bid Set Drawings and Specifications packages for Phase 1 and Phase 2 will be prepared as print-ready full-sized drawings (1 set) and a pdf set of the drawings in full-size and half-size; One set of master specifications on both 8 1/2"x11" paper unbound and in digital form. All deliverables will be in two separate packages for Phase 1 and Phase 2 work.

ADDITIONAL OPTIONAL TASKS

We have included several optional tasks for the City to consider in case they become needed. These tasks are:

Task 6 – Potholing: We have included a budgetary item due to unknown number of utilities.

Task 7 – Title report and easement legal descriptions: We have included a budgetary item based on an assumed number of five due to the unknown number of easements that may be required.

Task 8 – Trenchless Installation Evaluation and Report: If trenchless installation of the pipeline under Mill Creek Channel is selected, we will request Brierley and Associates, our tunneling subconsultant, to evaluate and recommend the tunneling method to be used.

Task 9 – Additional Geotechnical Investigations if needed.

ASSUMPTIONS

The Scope of Work developed above and the associated labor hour effort to complete the work was based on the following assumptions:

1. The duration of the project design will be approximately 14 months from receipt of the Notice to Proceed.
2. No additional conditional assessment of the existing Tate WTP raw water transmission line will be needed.
3. Scour analysis of Mill Creek Channel is not included. We understand that a scour analysis is available from SBCFCD.
4. Traffic control plans are not included. The City will provide traffic control plans for inclusion.
5. City will provide the following services as needed during the project:
    a. Provide potholing and/or jet-tracing of any utilities with uncertain locations. We have included a budgetary item under Optional Task 7 for $20,000 for potholing;
    b. Provide plan reviews of intermediate submittals in a timely manner (assumed to be 2-weeks);
    c. Provide bid documents to prospective bidders (including printing and the bid form template) and bid the projects;
    d. Provide cost data from recent projects for use in preparation of engineer's cost estimates;
    e. Pay for costs associated with dry utility company (gas, power, communication) design fees.
    f. Apply for and pay the fees associated with obtaining permits.
6. Costs incurred by the utility companies for their design work will be paid for directly by the City.
7. The bidding documents will use City's Front End (Division 0). The City will provide the latest version of the their Front End to Carollo for review and co-ordination with the rest of the technical specifications.

8. A detailed SWPPP is outside of the scope of work and will be prepared by the Contractor.
9. Printing of Bid Sets for Bidding will be provided by City as needed.
10. Bid services are not included in the Scope of Work.
11. Public Outreach will be provided by City.

Attachment A includes a preliminary List of Drawings for Phase 1 and Phase 2 design. Total sheet count is 58.

Attachment A
Preliminary List of Drawings – Phase 1

SHEET No.	Drawing Title	No. of Drawings
	GENERAL	**4**
G-1	COVER SHEET, VICINITY, AND LOCATION MAP	1
G-2	DRAWING INDEX	1
G-3	LEGEND, SYMBOLS, AND ABBREVIATIONS	1
G-4	KEY PLAN, STAGING AREA, AND SURVEY CONTROL DATA	1
	CIVIL	**7**
GC-1	GENERAL CIVIL NOTES, LEGEND, AND SYMBOLS	1
GC-2	CIVIL STANDARD DETAILS 1	1
GC-3	CIVIL STANDARD DETAILS 2	1
C-1	TRANSMISSION PIPELINE PLAN AND PROFILE - 1	1
C-2	TRANSMISSION PIPELINE PLAN AND PROFILE - 2	1
C-3	BOX STRUCTURE SITE PLAN, SECTIONS, AND DETAILS	1
C-4	MILL CREEK CHANNEL CROSSING DETAILS	1
	STRUCTURAL	**5**
GS-1	GENERAL STRUCTURAL NOTES	1
GS-2	STANDARD STRUCTURAL DETAILS - 1	1
GS-3	STANDARD STRUCTURAL DETAILS - 2	1
S-1	BOX STRUTURE REPLACEMENT PLAN	1
S-2	BOX STRUTURE REPLACEMENT SECTIONS AND DETAILS	1
	Total Number of Drawings	**16**

Attachment A
Preliminary List of Drawings – Phase 2

SHEET No.	Drawing Title	No. of Drawings
	GENERAL	**4**
G-1	COVER SHEET, VICINITY, AND LOCATION MAP	1
G-2	DRAWING INDEX	1
G-3	LEGEND, SYMBOLS, AND ABBREVIATIONS	1
G-4	OVERALL SITE PLAN	1
	CIVIL	**12**
GC-1	GENERAL CIVIL NOTES, LEGEND, AND SYMBOLS	1
GC-2	STANDRD CIVIL DETAILS – 1	1
GC-3	STANDRD CIVIL DETAILS – 2	1
C-1	TRANSMISSION PIPELINE PLAN AND PROFILE - 1	1
C-2	TRANSMISSION PIPELINE PLAN AND PROFILE - 2	1
C-3	TRANSMISSION PIPELINE PLAN AND PROFILE - 3	1
C-4	CRAFTON TRANSMISSION PIPELINE PLAN AND PROFILE - 4	1
C-5	VALVE VAULT/FLOWMETER VAULT PLANS	1
C-6	VALVE VAULT/METER VAULT SECTIONS	1
C-7	CRAFTON VALVE/FLOWMETER VAULT PLANS	1
C-8	CRAFTON VALVE/FLOWMETER VAULT SECTIONS	1
C-9	MISCELLANEOUS PIPELINE CONNECTION DETAILS	1
	STRUCTURAL	**6**
GS-1	GENERAL STRUCTURAL NOTES	1
GS-2	STANDARD STRUCTURAL DETAILS - 1	1
GS-3	STANDARD STRUCTURAL DETAILS - 2	1
S-1	VALVE/FLOWMETER VAULT PLANS AND SECTIONS	1
S-2	CRAFTON VALVE/FLOWMETER VAULT PLANS AND SECTIONS	1
S-3	STRUCURAL DETAILS	1
	MECHANICAL	**5**
GM-1	MECHANICAL GENERAL NOTES	1
GM-2	STANDARD MECHANICAL DETAILS – 1	1

SHEET No.	Drawing Title	No. of Drawings
M-1	VALVE/FLOWMETER PLAN AND SECTION	1
M-2	CRAFTON VALVE/FLOWMETER PLAN AND SECTION	1
M-3	MISCELLANEOUS MECHANICAL DETAILS	1
	ELECTRICAL	**9**
GE-1	ELECTRICAL LEGEND	1
GE-2	ELECTRICAL GENERAL NOTES	1
GE-3	TYPICAL ELECTRICAL DETAILS - 1	1
GE-4	TYPICAL ELECTRICAL DETAILS - 2	1
E-1	ELECTRICAL SITE PLAN	1
E-2	VALVE/FLOWMETER ELECTRICAL PLAN	1
E-3	CRAFTON VALVE/FLOWMETER ELECTRICAL PLAN	1
E-4	POWER AND CONTROL RISERS	1
E-5	SCHEDULES AND SCHEMATICS	1
	INSTRUMENTATION	**6**
GN-1	PROCESS AND INSTRUMENTATION LEGEND - 1	1
GN-2	PROCESS AND INSTRUMENTATION LEGEND - 2	1
GN-3	TYPICAL INSTRUMENTATION DETAILS - 1	1
GN-4	TYPICAL INSTRUMENTATION DETAILS - 2	1
N-1	BLOCK DIAGRAM	1
N-2	P&ID	1
	Total Number of Drawings	**42**

EXHIBIT "B"

COST PROPOSAL

[ATTACHED]

EXHIBIT "D"

WORKERS' COMPENSATION INSURANCE CERTIFICATION

Every employer, except the State, shall secure the payment of compensation in one or more of the following ways:

(a) By being insured against liability to pay compensation by one or more insurers duly authorized to write compensation insurance in this State.

(b) By securing from the Director of Industrial Relations, a certificate of consent to self-insure, either as an individual employer, or as one employer in a group of employers, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his or her employees.

CHECK ONE

☑ I am aware of the provisions of Section 3700 of the Labor Code which requires every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code, and I will comply with such provisions before commencing the performance of the work and activities required or permitted under this Agreement. (Labor Code §1861).

☐ I affirm that at all times, in performing the work and activities required or permitted under this Agreement, I shall not employ any person in any manner such that I become subject to the workers' compensation laws of California. However, at any time, if I employ any person such that I become subject to the workers' compensation laws of California, immediately I shall provide the City with a certificate of consent to self-insure, or a certification of workers' compensation insurance.

I certify under penalty of perjury under the laws of the State of California that the information and representations made in this certificate are true and correct.

CAROLLO ENGINEERING, INC.

By: _____ Date: Apr 13, 2022

Graham J.G. Juby, Senior Project Manager

Carollo Engineers Agreement.PS-1.1.FY21-0090

Final Audit Report 2022-04-13

Created:	2022-04-13
By:	Eric M. Mills (emills@carollo.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA-v884IAko8L1MDkJJu0GDVrUigOOPfWa

"Carollo Engineers Agreement.PS-1.1.FY21-0090" History

Document created by Eric M. Mills (emills@carollo.com)
2022-04-13 - 2:32:36 PM GMT- IP address: 24.205.114.11

Document e-signed by Eric M. Mills (emills@carollo.com)
Signature Date: 2022-04-13 - 2:37:03 PM GMT - Time Source: server- IP address: 24.205.114.11

Document emailed to Graham Juby (gjgjuby@carollo.com) for signature
2022-04-13 - 2:37:05 PM GMT

Email viewed by Graham Juby (gjgjuby@carollo.com)
2022-04-13 - 3:25:58 PM GMT- IP address: 68.111.94.245

Document e-signed by Graham Juby (gjgjuby@carollo.com)
Signature Date: 2022-04-13 - 3:28:27 PM GMT - Time Source: server- IP address: 68.111.94.245

Agreement completed.
2022-04-13 - 3:28:27 PM GMT

CITY OF REDLANDS

Carollo Fee Estimate

Tate Water Treatment Plant Raw Water Influent Line Engineering Project

Task No.	TASK DESCRIPTION	Senior Professional	Project Manager	Lead Professional QA/QC	Project Professional	Professional	Assistant Professional	CAD Technician	Office Support	TOTAL HOURS	LABOR COST	Project Equipment and Communication Expense [PECE] ($13.00 per labor hour)	OTHER DIRECT COSTS	Subconsultants	Markup on ODCs and Subconsultants	TOTAL PROJECT FEE
	Hourly Billing Rate	$288	$265	$265	$245	$220	$180	$144	$120							
1.0	**PROJECT MANAGEMENT AND MEETINGS**	**28**	**62**	**38**	**68**	**0**	**0**	**0**	**14**	**210**	**$ 52,904**	**$ 2,730**	**$ 900**	**$ -**	**$ 90**	**$ 56,624**
A	Monthly invoices and progress reporting		8		14				4	26	$ 6,030	$ 338	$ 200		$ 20	$ 6,588
B	Attend monthly meetings (assume 12 meetings, 90 minutes each)	14	24	18	24				4	84	$ 21,522	$ 1,092	$ 200		$ 20	$ 22,834
C	Attend in-person review meetings at 30%, 60%, 90%, and 100% design level (assume 6 meetings)	14	30	20	30				6	100	$ 25,352	$ 1,300	$ 500		$ 50	$ 27,202
D	Quality Assurance and Quality Control (Built into Task 5.0-D)									0	$ -	$ -			$ -	$ -
2.0	**ALTERNATIVE EVALUATIONS**	**12**	**58**	**66**	**108**	**88**	**0**	**66**	**18**	**416**	**$ 93,800**	**$ 5,408**	**$ 1,500**	**$ -**	**$ 150**	**$ 100,858**
A	Review existing condition assessment report and other related documents	2	8	8	8			8	2	36	$ 8,168	$ 468			$ -	$ 8,636
B	Evaluation of trenched and trenchless pipe installation methods	2	8	16	12			8	1	47	$ 11,148	$ 611	$ 500		$ 50	$ 12,309
C	Evaluate feasibility of alternatives including life-cycles costs	1	8	8	8			8	2	35	$ 7,880	$ 455			$ -	$ 8,335
D	Hydraulics	1	4	4	12	40		4	1	66	$ 14,844	$ 858	$ 500		$ 50	$ 16,252
E	Water Quality		2	2	4				1	9	$ 2,160	$ 117			$ -	$ 2,277
F	Foundations		4	8	8			8	1	29	$ 6,412	$ 377			$ -	$ 6,789
G	Regulatory constraints	2	8	4	16	24			2	56	$ 13,196	$ 728			$ -	$ 13,924
H	Prepare Technical Memorandum No. 1 and presentation for pipeline alternatives (TM-01)	4	16	16	40	24		30	8	138	$ 29,992	$ 1,794	$ 500		$ 50	$ 32,336
3.0	**SITE SURVEY AND BASE MAP**	**1**	**6**	**0**	**6**	**0**	**0**	**22**	**2**	**37**	**$ 6,756**	**$ 481**	**$ -**	**$ 44,950**	**$ 4,495**	**$ 56,682**
A	Prepare a site survey	1	2		2			8	2	15	$ 2,700	$ 195		$ 44,950	$ 4,495	$ 52,340
B	Prepare field survey to establish boundaries		2		2			2		6	$ 1,308	$ 78			$ -	$ 1,386
C	Potholing of existing utilities including surveys of potholes (see Optional Task 8)									0	$ -	$ -			$ -	$ -
D	Jet tracing of gravity utilities including survey (Jet Tracing will be performed by the City if needed)									0	$ -	$ -			$ -	$ -
E	Establish local survey monuments (at least 3 survey control monuments)		2		2			4		8	$ 1,596	$ 104			$ -	$ 1,700
F	Prepare an AutoCAD base map for use in planning and design							8		8	$ 1,152	$ 104			$ -	$ 1,256
4.0	**GEOTECHNICAL INVESTIGATIONS**	**1**	**2**	**4**	**4**	**0**	**0**	**0**	**1**	**12**	**$ 2,978**	**$ 156**	**$ -**	**$ 59,933**	**$ 5,993**	**$ 69,060**
A	Perform geotechnical investigations, borings, slope stability, and report	1	2	4	4				1	12	$ 2,978	$ 156		$ 59,933	$ 5,993	$ 69,060
5.0	**FINAL ENGINEERING (Phase 1 and 2)**	**10**	**216**	**248**	**292**	**232**	**212**	**972**	**100**	**2,282**	**$ 438,548**	**$ 29,666**	**$ 3,500**	**$ -**	**$ 350**	**$ 472,064**
A	Prepare Final design plans, specifications and construction cost estimates (30% design level)	2	80	40	80	80	80	300	20	682	$ 129,576	$ 8,866	$ 1,000		$ 100	$ 139,542
B	Prepare Final design plans, specifications and construction cost estimates (60% design level)	2	60	60	80	80	80	300	20	682	$ 129,576	$ 8,866	$ 1,000		$ 100	$ 139,542
C	Prepare Final design plans, specifications and construction cost estimates (90% design level)	2	60	60	80	60	40	300	20	622	$ 117,976	$ 8,086	$ 1,000		$ 100	$ 127,162
D	Internal Check of Plans and Specs (QA/QC)	2	4	80	24			12	4	126	$ 30,924	$ 1,638			$ -	$ 32,562
E	Prepare Final design plans, specifications and construction cost estimates (100% final)	2	8	8	24	12		40	24	118	$ 21,976	$ 1,534	$ 500		$ 50	$ 24,060
F	Prepare Separate Bid Sets (Phase 1 and Phase 2)		4		4		12	20	12	52	$ 8,520	$ 676			$ -	$ 9,196
	TOTAL FOR ALL TASKS (TASKS 1-5)	**52**	**344**	**356**	**478**	**320**	**212**	**1,060**	**135**	**2,957**	**$ 594,986**	**$ 38,441**	**$ 5,900**	**$ 104,883**	**$ 11,078**	**$ 755,288**
	ADDITIONAL OPTIONAL TASKS															
6.0	Potholing if needed (budgetary number due to unknown number of utilities)		2	2				8	1	13	$ 2,332	$ 169		$ 20,000	$ 2,000	$ 24,501
7.0	Title Report and Easement Legal Description (assume 5@$3,500 each)		2	2	2	0	0	8	1	15	$ 2,822	$ 195	$ -	$ 17,500	$ 1,750	$ 22,267
8.0	Trenchless Installation Evaluation and Report by Brierley (if trenchless option is selected)		2	2	8			8	1	21	$ 4,292	$ 273		$ 25,000	$ 2,500	$ 32,065
9.0	Additional Geotechnical Investigations/Trenching (if needed)		2		2			2	1	7	$ 1,428	$ 84		$ 8,235	$ 824	$ 10,571
	TOTAL OPTIONAL TASKS (TASKS 6-10)	**0**	**8**	**6**	**12**	**0**	**0**	**26**	**4**	**56**	**$ 10,874**	**$ 637**	**$ -**	**$ 62,500**	**$ 6,250**	**$ 80,261**
	TOTAL INCLUDING OPTIONAL TASKS (TASKS 1-9)	**52**	**352**	**362**	**490**	**320**	**212**	**1,086**	**139**	**3,013**	**$ 605,860**	**$ 39,078**	**$ 5,900**	**$ 167,383**	**$ 17,328**	**$ 835,549**

FIRST AMENDMENT TO AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This first amendment ("First Amendment") to the agreement for Engineering services related to the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project dated April 19, 2022 ("Agreement"), by and between the City of Redlands, a municipal corporation ("City"), and Carollo Engineers, Inc. ("Consultant"), is made and entered into this 3rd day of October, 2023.

RECITALS

WHEREAS, it is the desire of the City and Consultant to amend their existing Agreement, specifically to extend the contract term by twelve (12) months to October 18, 2024.

NOW, THEREFORE, for good and valuable consideration in the receipt of which is hereby acknowledged City and Consultant agree as follows:

AMENDMENT

Section 1. Section 4.2 of Article 4 ("Performance of Services") of the Agreement, is hereby amended to read as follows:

"4.2 The term of this Agreement shall be for a period of thirty (30) months commencing as of the Effective Date, unless terminated earlier as provided herein."

Section 2. All other provisions of the Agreement shall remain unchanged by this First Amendment and in effect.

IN WITNESS WHEREOF, the parties have executed this First Amendment, to be effective as of October 3, 2023.

CITY OF REDLANDS

Eddie Tejeda, Mayor

Carollo Engineers, Inc.

By: _____

Graham J.G. Juby, Senior Project Manager

ATTEST:

Jeanne Donaldson, City Clerk

SECOND AMENDMENT TO AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This second amendment ("Second Amendment") to the agreement for Engineering services related to the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project dated April 19, 2022 ("Agreement"), by and between the City of Redlands, a municipal corporation ("City"), and Carollo Engineers, Inc., a Delaware corporation ("Consultant"), is made and entered into this 1st day of October, 2024.

RECITALS

WHEREAS, it is the desire of the City and Consultant to amend their existing Agreement, specifically to extend the contract term by twelve (12) months to October 18, 2025.

NOW, THEREFORE, City and Consultant agree as follows:

AGREEMENT

Section 1. Section 4.2 of Article 4 ("Performance of Services") of the Agreement, entitled is hereby amended to read as follows:

"4.2 The term of this Agreement shall be for a period of forty-two (42) months commencing as of the Effective Date, unless terminated earlier as provided herein."

Section 2. All other provisions of the Agreement shall remain unchanged by this Second Amendment and in effect.

IN WITNESS WHEREOF, the parties have executed this Second Amendment, to be effective as of October 1, 2024.

CITY OF REDLANDS

Eddie Tejeda, Mayor

CAROLLO ENGINEERS, INC.

By: _____

Graham J.G. Juby, Senior Project Manager

ATTEST:

Jeanne Donaldson, City Clerk

THIRD AMENDMENT TO AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This third amendment ("Third Amendment") to the agreement for Engineering services related to the Tate Water Treatment Plant Raw Water Influent Pipeline Replacement Project dated April 19, 2022 ("Agreement"), by and between the City of Redlands, a municipal corporation ("City"), and Carollo Engineers, Inc., a Delaware corporation ("Consultant"), is made and entered into this 2nd day of September, 2025.

RECITALS

WHEREAS, it is the desire of the City and Consultant to amend their existing Agreement, specifically to extend the contract term by twelve (12) months to October 18, 2026.

NOW, THEREFORE, City and Consultant agree as follows:

AGREEMENT

Section 1. Article 4 of the Agreement, entitled "Performance of Services," is hereby amended to read as follows:

"4.2 The term of this Agreement shall be for a period of fifty-four (54) months commencing as of the Effective Date, unless terminated earlier as provided herein."

Section 2. All other provisions of the Agreement shall remain unchanged by this Third Amendment and in effect.

IN WITNESS WHEREOF, the parties have executed this Third Amendment, to be effective as of September 2, 2025.

CITY OF REDLANDS

Mario Saucedo, Mayor

CARROLLO ENGINEERS, INC.

By: _____

Graham J.G. Juby, Senior Project Manager

ATTEST:

Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. I13.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve a Professional Services Agreement with Biggs Cardosa Associates, Inc. for conceptual engineering design of the Citrus Avenue and Redlands High School Crossing Project for an amount not to exceed $216,482; approve a Cooperative Agreement with Redlands Unified School District; re-designate a portion of the current $1,500,000 budgeted in the Arterial Street Fund 252 to the Local Transportation Fund 209 and Measure I Fund 210; and determine that approval of these agreements is not subject to environmental review under Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act (Municipal Utilities and Engineering Director Heredia)

MOTION:

If the City Council determines that staff recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that approval of these Agreements is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act;

2. I move that the City Council approve a Professional Services Agreement with Biggs Cardosa Associates, Inc. for conceptual engineering design services for the Citrus Avenue and Redlands High School Crossing Project in an amount not to exceed $216,482;

3. I move that the City Council approve a Cooperative Agreement with the Redlands Unified School District; and

4. I move that the City Council re-designate a portion of the current $1,500,000 budgeted in the Arterial Street Fund 252 to the Local Transportation Fund 209 and Measure I Fund 210.

RECOMMENDATION:

Staff recommends that the City Council determine that approval of these Agreements is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act. Staff further recommends that the City Council approve a Professional Services Agreement with Biggs Cardosa Associates, Inc. (BCA) for conceptual engineering design services for the Citrus Avenue and Redlands High School Crossing Project for an amount not to exceed $216,482; approve a Cooperative Agreement with the Redlands Unified School District; and re-designate a portion of the current $1,500,000 budgeted in the Arterial Street Fund 252 to the Local Transportation Fund 209 and Measure I Fund 210.

DISCUSSION:

The City of Redlands is seeking professional engineering consulting services to evaluate grade-separated pedestrian crossing alternatives along Citrus Avenue between the two campuses of Redlands High School. Throughout the school day, hundreds of students, faculty, and staff cross Citrus Avenue between class periods, creating frequent interactions between pedestrians and vehicular traffic despite the existing pedestrian-activated traffic control measures. The current at-grade crossing presents ongoing safety and operational concerns due to high pedestrian volumes, driver inattentiveness, traffic delays, and impacts to emergency response vehicles. This project is intended to improve pedestrian safety, reduce vehicle-pedestrian conflicts, minimize traffic congestion, improve emergency vehicle access, enhance bicycle and pedestrian connectivity between the campuses, and identify a constructible and financially feasible long-term transportation solution.

The selected consultant will provide all professional engineering services necessary to develop and evaluate three conceptual alternatives consisting of two underpass options and one pedestrian/bicycle overpass. The scope of work includes review of available studies, utility information, traffic data, and existing conditions; field investigations; evaluation of roadway, pedestrian, bicycle, drainage, utility, and traffic conditions; and identification of project constraints and opportunities. Each conceptual alternative will incorporate roadway improvements, pedestrian and bicycle facilities, drainage and stormwater improvements, lighting and security features, ADA-compliant accessibility, utility impacts and relocations, preliminary right-of-way and easement requirements, construction staging considerations, and preliminary construction cost estimates. The consultant will also evaluate environmental clearance requirements and anticipated permitting needs to support future project implementation.

Throughout the conceptual design process, the consultant will coordinate with the Redlands Unified School District, Redlands High School administration, students and parents, adjacent businesses and property owners, and other stakeholders identified by the City. Upon completion of the evaluations and stakeholder outreach, the consultant will prepare a technical memorandum summarizing the alternatives, associated benefits and constraints, environmental considerations, preliminary right-of-way requirements, estimated construction costs, and a recommended preferred alternative. The City will use this information to select a preferred grade-separated crossing alternative for advancement into final design and future construction.

On June 25, 2026, MUED staff issued a Request for Proposals (RFP) for engineering design services necessary as described above. On July 21, 2026, proposals were received from the following four (4) firms:

1. Albert A. Webb Associates, Riverside, CA
2. AYCE Consulting Engineers, Inc., Santa Ana, CA
3. Biggs Cardosa Associates, Inc., Orange, CA
4. TKE Engineering, Inc., Riverside, CA

Pursuant to Chapter 2.16.180 of the Redlands Municipal Code, an evaluation committee conducted a comprehensive review of the proposals and ranked each firm based on its demonstrated competence, relevant experience, and professional qualifications in accordance with the evaluation criteria established in the RFP. Following the evaluation, BCA was determined to be the most qualified firm to provide the requested conceptual engineering design services. Accordingly, staff recommends that the City Council approve a Professional Services Agreement with BCA, Inc. in an amount not to exceed $216,482.

As the City intends to improve pedestrian crossings along Citrus Avenue to enhance pedestrian safety and connectivity between the north and south campuses of Redlands High School, MUED staff has coordinated with the Redlands Unified School District regarding the proposed improvements, and the School District has expressed interest in participating in the Project and sharing a portion of the Project costs. Approximately 76.9 percent of the total Project cost will be reimbursed through SBCTA's Measure I Arterial Fund, with the remaining 23.1 percent local share to be divided equally between the City and the School District. The School District's contribution is estimated at $25,003.50. MUED will lead the project and coordinate with the School District throughout project development and implementation to ensure the improvements meet the needs of both campuses and the surrounding community.

The proposed Citrus Avenue Grade-Separated Pedestrian Crossing Project is eligible for funding through the Development Impact Fee (DIF) Program because it addresses an identified transportation infrastructure need associated with existing and future development and provides a Citywide transportation benefit. The project will improve pedestrian and bicycle connectivity between the two Redlands High School campuses, enhance pedestrian safety, reduce vehicle-pedestrian conflicts, improve traffic operations, and minimize delays to emergency response vehicles. By providing a long-term, grade-separated crossing facility, the project will increase the capacity, safety, and efficiency of the City's transportation network and support the City's ability to accommodate existing and future transportation demands. Accordingly, the project is consistent with the purpose of DIF-funded improvements to provide or enhance transportation facilities necessary to serve the increased demand generated by development.

Approval of these Agreements is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act, as there is no possibility that this action will result in a significant impact on the environment.

ALTERNATIVES:

The City Council may choose not to approve one or both Agreements and provide alternative direction to staff.

STRATEGIC PLAN:

The Project supports Strategic Plan Priority D, Strategic Objective 3. Infrastructure: Engineer and construct transportation facilities to accommodate all potential users - motorists, cyclists, and pedestrians.

SUBMITTED BY:
Monica Heredia, Municipal Utilities and Engineering Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
Dana Abramovitz-Daniel, Procurement Manager
James Garland, Finance Director

PREPARED BY:
Goutam Dobey, City Engineer

FISCAL IMPACT

Fiscal Year: FY 2026/27

Revenue Generating: No

Budgeted Y/N: Yes

Account No.: Multiple

Additional Appropriation Required: No

Discussion:

The FY 2026-27 MUED Arterial Street Construction Budget (Fund 252) includes $1,500,000 for the Project. Of this amount, $216,482 was established for the design portion of this project. The remaining $1,283,518 will be used for construction and other expenditures. In order to appropriately record expenditure and revenue activity with these special revenue funds, re-designating a portion of the current $1,500,000 budgeted in the Arterial Street Fund 252 to the Local Transportation Fund 209 and Measure I Fund 210 will be required. The updated budget re-designation will be as follows:

209410-4901 (Transfer In) for $191,478.50
209410-4405 (Cost Recovery) for $25,003.50
210410-9901 (Transfer Out) for $166,475
252400-9901 (Transfer Out) for $25,003.50
210410-4007 (Measure I Arterial Revenue) for $166,475
209410-8501 (Other Betterment's and Improvements) for $216,482

The Project cost has been budgeted in the MUED budget for Fiscal Year 2026/27, and costs will be shared with the Redlands Unified School District. The following is the funding breakdown:

Measure I Arterial Fund: 76.9%
City Development Share: 23.1% (50-50 split between City and School District)

			LOCAL DEVELOPMENT SHARE	
PHASE	**TOTAL COST**	**MEASURE I**	**CITY**	**SCHOOL DISTRICT**
Conceptual Design	$216,482	$166,475	$25,003.50	$25,003.50
TOTAL	**$216,482**	**$166,475**	**$25,003.50**	**$25,003.50**

Attachments

A_Biggs_Cardosa_Professional_Services_Agreement.pdf
B_Cooperative_Agreement_with_RUSD.pdf

AGREEMENT TO PERFORM PROFESSIONAL SERVICES

This agreement for the provision of Conceptual Engineering Design Services of the Citrus Avenue and Redlands High School Crossing Project ("Agreement") is made and entered in this 6th day of October, 2026 ("Effective Date"), by and between the City of Redlands, a municipal corporation ("City") and Biggs Cardosa Associates, Inc. a California corporation ("Consultant"). City and Consultant are sometimes individually referred to herein as a "Party" and, together, as the "Parties." In consideration of the mutual promises contained herein, City and Consultant agree as follows:

ARTICLE 1 – ENGAGEMENT OF CONSULTANT

1.1 City hereby engages Consultant to provide Conceptual Engineering Design of the Citrus Avenue and Redlands High School Crossing Project services for City (the "Services").

1.2 The Services shall be performed by Consultant in a professional manner, and Consultant represents that it has the skill and the professional expertise necessary to provide the Services to City at a level of competency presently maintained by other practicing professional consultants in the industry providing like and similar types of Services.

ARTICLE 2 – SERVICES OF CONSULTANT

2.1 The Services that Consultant shall perform are more particularly described in Exhibit "A," titled "Scope of Services," which is attached hereto and incorporated herein by this reference.

2.2 Consultant shall comply with applicable federal, state and local laws and regulations in the performance of this Agreement including, but not limited to, any applicable State prevailing wage laws.

ARTICLE 3 – RESPONSIBILITIES OF CITY

3.1 City designates Monica Heredia, Municipal Utilities and Engineering Department Director, as City's representative with respect to performance of the Services, and such person shall have the authority to transmit instructions, receive information, interpret and define City's policies and decisions with respect to performance of the Services.

ARTICLE 4 – PERFORMANCE OF SERVICES

4.1 Consultant shall perform and complete the Services in a prompt and diligent manner in accordance with the schedule set forth in Exhibit "B," titled "Project Schedule," which is attached hereto and incorporated herein by reference.

4.2 Consultant shall complete the Services by June 30, 2027, unless the Services are terminated earlier as provided for herein.

4.3 If Consultant's Services include deliverable electronic visual presentation materials, such materials shall be delivered in a form, and made available to City, consistent with City Council-adopted policy for the same. It shall be the obligation of Consultant to obtain a copy of such policy from City staff.

ARTICLE 5 – PAYMENTS TO CONSULTANT

5.1 Compensation: Total compensation for Consultant's performance of the Services shall not exceed the amount of Two Hundred Sixteen Thousand Four Hundred Eighty-two dollars ($216,482). City shall pay Consultant on a time and materials basis up to the not-to-exceed amount in accordance with Exhibit "C," titled "Fee Proposal," which is attached hereto and incorporated herein by reference.

5.2 Consultant shall submit monthly invoices to City describing the Services performed during the preceding month. Consultant's invoices shall include a brief description of the Services performed, the dates the Services were performed, the number of hours spent and by whom, and a description of reimbursable expenses related to the Services. City shall pay Consultant no later than thirty (30) days after receipt and approval by City of Consultant's invoice.

5.3 Any notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a Party may provide notice in accordance with this section:

CITY:	CONSULTANT:
City Clerk	Eric Pheifer, Principal/Vice President
City of Redlands	Biggs Cardosa Associates, Inc.
35 Cajon Street	500 S. Main Street, Suite 1200
P.O. Box 3005 (mailing)	Orange, CA 92868
Redlands, CA 92373	epheifer@biggscardosa.com
jdonaldson@cityofredlands.org	Phone: (714) 352-8312
Phone: (909) 798-7531	Fax: (408) 296-8114

ARTICLE 6 – INSURANCE AND INDEMNIFICATION

6.1 The following insurance coverage required by this Agreement shall be maintained by Consultant for the duration of its performance of the Services. Consultant shall not perform any Services unless and until the required insurance listed below is obtained by Consultant. Consultant shall provide City with certificates of insurance and endorsements

evidencing such insurance prior to commencement of the Services. Insurance policies shall include a provision prohibiting cancellation or modification of the policy except upon thirty (30) days prior written notice to City.

A. Workers' Compensation and Employer's Liability insurance in the amount that meets statutory requirements with an insurance carrier acceptable to City, or certification to City that Consultant is self-insured or exempt from the workers' compensation laws of the State of California. Consultant shall execute and provide City with Exhibit "D," titled "Workers' Compensation Insurance Certification," which is attached hereto and incorporated herein by this reference, prior to performance of the Services.

B. Comprehensive General Liability insurance with carriers acceptable to City in the minimum amount of One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) aggregate, for public liability, property damage and personal injury is required. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

C. Consultant shall secure and maintain professional liability insurance throughout the term of this Agreement in the amount of One Million Dollars ($1,000,000) per claim made.

D. Business Auto Liability coverage, with minimum limits of One Million Dollars ($1,000,000) per occurrence, combined single limit bodily injury liability and property damage liability. This coverage shall include all Consultant owned vehicles used in connection with Consultant's provision of the Services, hired and non-owned vehicles, and employee non-ownership vehicles. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

E. Consultant is expressly prohibited from assigning or subcontracting any of the Services without the prior written consent of City. In the event of mutual agreement by the Parties to assign or subcontract a portion of the Services, Consultant shall add such assignee or subcontractor as an additional insured to the insurance policies required hereby and provide City with the insurance endorsements prior to any Services being performed by the assignee or subcontractor.

6.2 Consultant shall defend, indemnify and hold harmless City and its elected and appointed officials, employees and agents from and against any and all claims, losses or liability, including attorneys' fees, arising from injury or death to persons or damage to property occasioned by any negligent act or omission by, or the willful misconduct of, Consultant, or its officers, employees and agents in performing the Services.

ARTICLE 7 – CONFLICTS OF INTEREST

7.1 Consultant covenants and represents that it does not have any investment or interest in any real property that may be the subject of this Agreement or any other source of income, interest in real property or investment that would be affected in any manner or degree by the performance of Consultant's Services. Consultant further covenants and represents that in the performance of its duties hereunder, no person having any such interest shall perform any Services under this Agreement.

7.2 Consultant agrees it is not a designated employee within the meaning of the Political Reform Act because Consultant:

A. Does not make a governmental decision whether to:

(i) approve a rate, rule or regulation, or adopt or enforce a City law;
(ii) issue, deny, suspend or revoke any City permit, license, application, certification, approval, order or similar authorization or entitlement;
(iii) authorize City to enter into, modify or renew a contract;
(iv) grant City approval to a contract that requires City approval and to which City is a party, or to the specifications for such a contract;
(v) grant City approval to a plan, design, report, study or similar item;
(vi) adopt, or grant City approval of, policies, standards or guidelines for City or for any subdivision thereof.

B. Does not serve in a staff capacity with City and in that capacity, participate in making a governmental decision or otherwise perform the same or substantially the same duties for City that would otherwise be performed by an individual holding a position specified in City's Conflict of Interest Code under Government Code section 87302.

7.3 In the event City determines that Consultant must disclose its financial interests, Consultant shall complete and file a Fair Political Practices Commission Form 700, Statement of Economic Interests, with the City Clerk's office pursuant to the written instructions provided by the City Clerk.

ARTICLE 8 – GENERAL CONSIDERATIONS

8.1 In the event any action is commenced to enforce or interpret any of the terms or conditions of this Agreement the prevailing Party shall, in addition to any costs and other relief, be entitled to the recovery of its reasonable attorneys' fees, including fees for the use of in-house counsel by a Party.

8.2 Consultant shall not assign any of the Services, except with the prior written approval of City and in strict compliance with the terms and conditions of this Agreement. Any assignment or attempted assignment without such prior written consent may, in the sole discretion of City, result in City's immediate termination of this Agreement.

8.3 Consultant is for all purposes under this Agreement an independent contractor and shall perform the Services as an independent contractor. Neither City nor any its agents shall have control over the conduct of Consultant or Consultant's employees, except as herein set forth. Consultant shall supply all necessary tools and instrumentalities required to perform the Services. Assigned personnel employed by Consultant are for its account only, and in no event shall Consultant or personnel retained by it be deemed to have been employed by City or engaged by City for the account of, or on behalf of City. Consultant shall have no authority, express or implied, to act on behalf of City in any capacity whatsoever as an agent, nor shall Consultant have any authority, express or implied, to bind City to any obligation.

8.4 This Agreement may be terminated by City, in its sole discretion, by providing not less than five (5) days prior written notice to Consultant of City's intent to terminate. If this Agreement is terminated by City, an adjustment to Consultant's compensation shall be made, but (1) no amount shall be allowed for anticipated profit or unperformed Services, and (2) any payment due Consultant at the time of termination may be adjusted to the extent of any additional costs to City occasioned by any default by Consultant. Upon receipt of a termination notice, Consultant shall immediately discontinue its provision of the Services and, within five (5) days of the date of the termination notice, deliver or otherwise make available to City, copies (in both hard copy and electronic form, where applicable) of project related data, design calculations, drawings, specifications, reports, estimates, summaries and such other information and materials as may have been accumulated by Consultant in performing the Services. Consultant shall be compensated on a pro-rata basis for Services completed up to the date of termination.

8.5 Consultant shall maintain books, ledgers, invoices, accounts and other records and documents evidencing costs and expenses related to the Services for a period of three (3) years, or for any longer period required by law, from the date of final payment to Consultant pursuant to this Agreement. Such books shall be available at reasonable times for examination by City at the office of Consultant.

8.6 This Agreement, including the Exhibits incorporated herein by reference, represents the entire agreement and understanding between the Parties as to the matters contained herein, and any prior negotiations, written proposals or verbal agreements relating to such matters are superseded by this Agreement. Except as otherwise provided for herein, any amendment to this Agreement shall be in writing, approved by City and signed by City and Consultant.

8.7 This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions. The Parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated only in the state courts located in San Bernardino County, California, and the federal courts located in Riverside County, California.

8.8 If one or more of the sentences, clauses, paragraphs or sections contained in this Agreement is declared invalid, void or unenforceable by a court of competent jurisdiction, the same shall be deemed severable from the remainder of this Agreement and shall not affect, impair or invalidate the remaining sentences, clauses, paragraphs or sections contained herein, unless to do so would deprive a Party of a material benefit of its bargain under this Agreement.

IN WITNESS WHEREOF, duly authorized representatives of City and Consultant have signed in confirmation of this Agreement.

CITY OF REDLANDS

By: _____
Mario Saucedo, Mayor

BIGGS CARDOSA ASSOCIATES, INC.

By: _____
Eric Pheifer, Principal/Vice President

ATTEST:

_____
Jeanne Donaldson, City Clerk

EXHIBIT "A"

SCOPE OF SERVICES

SCOPE OF SERVICES

The City intends to complete a detailed conceptual design and cost estimate for the Citrus Avenue and Redlands High School Crossing Project ("Project"). The Project will evaluate, develop, and design a pedestrian crossing improvement along Citrus Avenue between the north and south campuses of Redlands High School.

Throughout the school day, hundreds of students, faculty, and staff cross Citrus Avenue between class periods. Although the crossing is currently controlled by pedestrian-activated traffic control measures, conflicts between pedestrians and vehicular traffic continue to occur. The existing at-grade crossing presents safety concerns due to high pedestrian volumes, driver inattentiveness, traffic delays, and operational impacts to emergency response vehicles. The City desires to evaluate grade-separated crossing alternatives that improve pedestrian safety, maintain traffic operations, and provide a long-term transportation solution.

The primary objectives of the project are to:

- Improve pedestrian safety for students, faculty, and staff crossing Citrus Avenue.
- Reduce vehicle-pedestrian conflicts along the corridor.
- Minimize traffic congestion and operational delays caused by frequent pedestrian crossings.
- Improve emergency vehicle access and response times.
- Enhance bicycle and pedestrian connectivity between the two campuses.
- Develop a constructible and financially feasible grade-separated crossing solution.

EXISTING CONDITIONS AND OBSERVATIONS

The following existing conditions and observations have been made in preparation of this Scope of Services:

- Citrus Avenue is classified as a minor arterial in the city's roadway classification of the General Plan. Roadway right of way varies from 72' to 88' depending upon the typical section proposed. Assessor Parcel Maps show the current half-street right of way on the south side of the street is consistent at 39-feet from Church Street to University Street. The north side of Citrus Avenue is primarily a 44-foot half street right of way except fronting the residential homes west of Central Avenue.
- Citrus Avenue has an existing Class II bike lane – green painted extending from Church Street to University Street and extending easterly to Grove Street. To the west of Church Steet, the Class II bike lane joins a Class III bike lane.
- Citrus Avenue is also designated as a Truck Route from Wabash Avenue to the east of the school site to Orange Street, located west of the school site.
- Site observations show several underground utilities located within the project site area. Communication manholes were observed on the north side of Citrus Avenue at several location fronting the school. Sewer manholes were observed approximately at the center of Citrus Avenue in addition to water valves for fire hydrants and services to the school

observed near the center of the street. Edison had several vaults along the north side of Citrus Avenue within the school limits. Catch basins were at the intersection of University Street, at the intersection of Central Avenue, fronting the residential properties and at the intersection with Church Street large curb-opening basins were located on both sides of Citrus Avenue.

TASK 1 – PROJECT MANAGEMENT & ADMINISTRATION

This task includes Consultant's "day-to-day" management of the Project, and meetings with the City and external agencies.

1.1 Monthly Invoicing & Progress Reporting

The Consultant will submit invoices on a monthly basis in a format acceptable to the City that include hourly breakdowns per staff classification per task. A monthly progress report will also be included describing the progress per task.

Assumptions	This scope assumes that the Period of Performance will be up to six (6) months. Invoicing will be per task (e.g. Task 1 – Project Management & Administration). Further breakdown of subtasks (e.g. Task 1.1 Monthly Invoicing & Progress Reporting) is not anticipated.
Deliverables	Monthly Invoices & Progress Reports

1.2 Coordination & Meetings

The Consultant shall conduct regular meetings and coordination with the City's staff in monthly Project Development Team (PDT) meetings or technical and focused meetings as necessary. The Consultant shall be responsible for preparation of agendas and meeting minutes. PDT meetings will discuss project progress, issues, and action items. Technical meetings will be focused on specific technical issues (e.g. resolution of technical comments on the conceptual design).

With respect to external agencies, the Consultant shall specifically coordinate with:

- Redlands Unified School District.
- Redlands High School administration.
- Students and parents, as appropriate.
- Adjacent businesses and property owners.

Meetings with entities not noted above are expected to occur during the final design phase (e.g. meeting with affected third-party utilities).

Assumptions	The City will identify the necessary PDT members outside of the Consultant's team. Up to six (6) PDT meetings are included in this scope and are assumed to be conducted virtually. Up to two (2) technical workshops are anticipated to discuss the conceptual

	design and resolve comments. Those meetings are assumed to be conducted virtually. Up to two (2) meetings with Redlands Unified School District and Redlands High School administration are included in this scope and are anticipated to occur on-site. One (1) City Council meeting is anticipated to present the Feasibility Study Report. Students, parents, adjacent business and property owners, and the general public will be able to participate in this meeting. Extensive public outreach services to inform students, parents, adjacent businesses, property owners, etc. are not anticipated as part of this scope. The final design phase may require a public outreach consultant to host public workshops and prepare a project website, fact sheet, etc., but those services are not deemed essential for this phase of the Project.
Deliverables	PDT Meeting Agenda Packages PDT Meeting Minutes Technical Workshop Comment Resolution Logs City Council PPT Presentation

1.3 Project Schedule

The Consultant shall prepare and update the Project schedule on a monthly basis, or as needed. The Project schedule will include the Work Breakdown Structure in this Scope of Services, and significant tasks and milestones necessary to complete the Project. The critical path will be clearly depicted. Monthly schedule updates will show actual versus planned progress.

Assumptions	The project schedule will be developed in Microsoft Project. Monthly progress schedules will be delivered in PDF format and will be attached to invoice packages and included as part of PDT meeting agenda packages.
Deliverables	Baseline Project Schedule Monthly Progress Schedules

TASK 2 – DATA COLLECTION

This task primarily relates to collecting available record data, performing aerial survey, and preparing base mapping for use in conceptual design.

2.1 Record Data Collection & Review

The Consultant shall request, collect, assemble, and review all pertinent project information including roadway, utility, and traffic as-builts. City and Caltrans standards relevant to this

Project will be collected and reviewed. Available traffic data will be collected. All data collected by the Consultant will be assembled and made available to the City on a SharePoint site.

Assumptions	This scope assumes that the City will pay fees that may be required by external agencies to compile and transmit record data. The City will provide available vehicular traffic data on Citrus Avenue, and Redlands High School administration will provide data on number of students and pedestrian crossings of Citrus Avenue. Traffic counts and pedestrian counts are not anticipated as part of this scope, but would likely be required during final design. The purpose of the traffic data collection for this phase is to provide some text in the Feasibility Study related to Average Daily Traffic and number of pedestrian crossings, and no traffic reports are anticipated.
Deliverables	Project Data Collection File

2.2 Aerial Survey Base Mapping

The Consultant's field crews will establish ground control and perform an aerial survey of the site identified in the exhibit provided in the RFP. The survey will be conducted using a survey-grade, RTK-equipped unmanned aerial system (UAS). The final deliverables will consist of processed orthorectified aerial imagery georeferenced to California Coordinate System, Zone 5.

Assumptions	The limits of aerial survey will be along Citrus Avenue between Church Street and E Central Avenue with a swath of roughly 500 feet.
Deliverables	Georeferenced Orthomosaic Image High-Resolution Aerial Imagery Digital files suitable for incorporation into project exhibits, mapping, or coordination documents

2.3 Right of Way Base Mapping

The Consultant will perform research with the County of San Bernardino to acquire record maps and GIS data to prepare a Right of Way Base Map in DWG format. The base map will show parcel lines and APNs. The base mapping will be used to develop preliminary right of way requirements for the concept alternatives.

Assumptions	Ordering Title Reports and plotting easements that do not appear on record maps is not anticipated as part of this scope. The Right of Way Base Map will be developed based on record data. Field survey will be conducted during the final design phase to locate monuments, resolve boundaries, and update the Right of Way Base Map.
Deliverables	Right of Way Base Map

2.4 Utility Research and Base Mapping

The Consultant will utilize the Dig Alert website to determine the utility companies with facilities in the location of the proposed work. Consultant will work with the City to prepare Utility "A" Letters to be sent to these utility companies. Letters are anticipated to be prepared on City letterhead and can be sent via email either by the City or by the Consultant. An exhibit showing the approximate project limits will be attached to the letters. Record information received in response to the letters will be used to develop a utility base map in DWG format. The utility base map will be shown in the concept plans to identify potential strategies to relocate or protect-in-place during the subsequent final design phase.

Assumptions	If available, the City will provide their list of utility companies and contact information. Should any utility companies require a fee to process the as-built request and supply maps, this scope assumes that the City would pay those fees. This scope does not include potholing. It is assumed that potholing will be required for the subsequent final design phase.
Deliverables	Utility "A" Letters Utility Base Map Correspondence with Utility Companies

TASK 3 – CONCEPTUAL DESIGN

The Consultant shall develop and evaluate three conceptual alternatives, including:

- Undercrossing Alternative No. 1
- Undercrossing Alternative No. 2
- Pedestrian / Bicycle Overcrossing Alternative

Each alternative shall include:

- Review of available studies, plans, utility information, and traffic data.
- Information from site investigations and field reviews.
- Evaluation of existing roadways, pedestrians, bicycles, drainage, utility, and traffic conditions.
- Identification of constraints and opportunities affecting project development.
- Conceptual roadway improvements.
- Pedestrian facilities.
- Bicycle accommodations.
- Drainage and stormwater improvements (if needed).
- Lighting and security features.
- Accessibility and ADA compliance.
- Utility impacts and relocations.

- Preliminary right of way and easement requirements.
- Preliminary construction staging considerations.
- Preliminary construction cost estimates.

The conceptual design items noted above shall be of sufficient granularity to confirm feasibility and to formulate implementation recommendations for the final design phase. Concept plans and cost estimates are described in further detail below. Write-ups for the other items (above) will be included in the Feasibility Study Report.

3.1 Concept Plans

The Consultant will develop concept-level plans for each alternative. Conceptual plans shall be developed to a level sufficient to evaluate feasibility, benefits, impacts, and estimated costs. For each alternative, the plans are anticipated to include:

- Undercrossing / Overcrossing General Plan
- Undercrossing / Overcrossing Foundation Plan
- Site Plans / Street Improvement Plans
- Stage Construction / Traffic Handling Plans
- Right of Way Requirements

Plans will reference appropriate City, Caltrans, and SPPWC, where applicable. They will be developed in DWG format using a City-provided titleblock and delivered in PDF format. The Concept Plans will be attached to the Feasibility Study Report.

Site Plans / Street Improvement Plans: Consultant's Site Plans will show how the proposed alternatives join the on-site improvements. ADA paths of travel will be labeled with min/max slopes allowed and path widths. Street Improvements Plans will provide the existing street improvements along with signing and striping. The City's Traffic Engineer will provide input for each alternative as related to pedestrian crossings and striping for the Class II bike lane.

Stage Construction / Traffic Handling Plans: The Stage Construction / Traffic Handling Plan will provide how the general traffic will proceed through the construction zone in addition to how school personnel, student drop offs, student parking and pedestrian crossing will continue daily with as minimal disruption as possible. The City's Traffic Engineer will make recommendations to maintain safety of all pedestrians utilizing the crossings in Citrus Avenue.

Assumptions	This scope assumes that the preferred structure type for the undercrossing alternatives will be a cast-in-place or precast concrete box, and a prefabricated pedestrian truss bridge for the overcrossing alternative. Decisions about preferred structure types are assumed to be determined via sample photos and discussions, and preparation of additional General Plans showing multiple structure types for each alternative are not anticipated. Draft concept plans will undergo one round of City review, and the final concept plans will be developed. Additional rounds of reviews or additional third-party reviewers are not anticipated.

	The following assumptions were made with respect to total number of sheets: ▪ Undercrossing / Overcrossing General Plans: 3 ▪ Undercrossing / Overcrossing Foundation Plans: 3 ▪ Site Plans / Street Improvement Plans: 6 ▪ Stage Construction / Traffic Handling Plans: 6 ▪ Right of Way Requirements: 3 Confirmation of ownership and maintenance responsibility of the storm drain facilities will be confirmed. If the facilities are under SBCFCD, coordination will take place to determine their permitting requirements for the assessed alternative concepts. These will be noted in the Feasibility Study Report, and further coordination and permit applications will be undertaken during the final design phase.
Deliverables	Concept Plans

3.2 Preliminary Cost Estimates

Preliminary construction cost estimates will be developed for the three alternatives. Cost estimates will show estimated quantities and unit prices. Cost estimates will be prepared in Excel format and delivered in PDF format. Cost estimates will be attached to the Feasibility Study Report.

Assumptions	Line items and quantities will be based on rough order of magnitude estimates. Detailed quantity calculations are not anticipated for this phase of the project. Unit prices will be based on recent bids, Consultant's experience with similar projects, and Caltrans Contract Cost Data. Unit prices will include materials and labor. The use of RSMeans or other estimating methods and detailed breakdowns of labor and material costs are not anticipated. Draft preliminary construction cost estimates will undergo one round of City review, and the final preliminary construction cost estimates will be developed. It is assumed that the City is responsible for securing funding for both the feasibility and final design phases. Should the City desire Consultant's assistance in pursuing funding sources, Consultant will work with the City to develop a scope and fee for the extra work. It is assumed that all cost estimates will be agnostic to potential funding sources. Should the City require cost estimates to be subdivided based on specific requirements of funding agencies, Consultant will work with the City to assess the extra effort and, if necessary, develop a scope and fee for the extra work.
Deliverables	Preliminary Construction Cost Estimates

3.3 Renderings

Consultant will prepare renderings (i.e. photosimulations) for the conceptual alternatives. The proposed undercrossing or overcrossing will be modeled and superimposed on a picture of the existing conditions. These renderings will be included in the Feasibility Study Report, and can be presented to the project's stakeholders.

Assumptions	This scope assumes up to three (3) rendered still views, assumed to be one for each alternative. Consultant can provide additional views if needed, and can coordinate with the City on the additional scope/fee for that effort. City will select the preferred photos (ground or aerial) for use in the photosimulations. This scope does not assume renderings for multiple structure types or finish options. It is assumed that those elements will be determined through coordination meetings and samples, and the preferred structure types and aesthetics will be used in the renderings.
Deliverables	Renderings

TASK 4 – FEASIBILITY STUDY REPORT

The technical memorandum (Feasibility Study Report) will summarize:

- Alternative evaluations.
- Benefits and constraints.
- Environmental considerations.
- Right-of-way requirements.
- Construction costs.
- Recommended preferred alternative.

The Consultant shall provide recommendations regarding the appropriate environmental clearance pathway and anticipated permitting requirements.

Following completion of conceptual design and stakeholder review, the City will select one preferred alternative for advancement into final design.

Assumptions	The effort contained in this task is primarily to develop the Feasibility Study Report and prepare text to address existing conditions, alternative advantages/disadvantages, ADA compliance, etc. The effort to develop concept plans and preliminary construction cost estimates is contained under Task 3. Feasibility Study Report appendices will include concept plans and preliminary construction cost estimates developed in Task 3 along with any relevant data collected as part of Task 2. The Draft Feasibility Study Report will undergo one round of City review, and the Final Feasibility Study Report will be developed. It is assumed that the Final Feasibility Study Report will be presented to City Council.
Deliverables	Feasibility Study Report

EXHIBIT "B"
PROJECT SCHEDULE

Task Name	Duration	Start	Finish
Redlands High School Crossing	**188 days**	**Mon 10/12/26**	**Wed 6/30/27**
Key Milestones	**91 days**	**Mon 10/12/26**	**Tue 2/16/27**
Notice to Proceed	0 days	Mon 10/12/26	Mon 10/12/26
Conceptual Design Phase Completed	0 days	Tue 2/16/27	Tue 2/16/27
Task 1 - Project Management & Administration	**85 days**	**Mon 10/12/26**	**Fri 2/5/27**
Monthly Invoicing & Progress Reporting	85 days	Mon 10/12/26	Fri 2/5/27
Coordination & Meetings	85 days	Mon 10/12/26	Fri 2/5/27
Project Schedule Updates	85 days	Mon 10/12/26	Fri 2/5/27
Task 2 - Data Collection	**30 days**	**Mon 10/12/26**	**Fri 11/20/26**
Record Data Collection & Review	15 days	Mon 10/12/26	Fri 10/30/26
Aerial Survey Base Mapping	25 days	Mon 10/19/26	Fri 11/20/26
Right of Way Base Mapping	15 days	Mon 10/19/26	Fri 11/6/26
Utility Research & Base Mapping	25 days	Mon 10/19/26	Fri 11/20/26
Task 3 - Conceptual Design	**40 days**	**Mon 11/2/26**	**Fri 12/25/26**
Concept Plans	30 days	Mon 11/2/26	Fri 12/11/26
Preliminary Cost Estimates	10 days	Mon 12/14/26	Fri 12/25/26
Renderings	20 days	Mon 11/16/26	Fri 12/11/26
Task 4 - Feasibility Study Report	**163 days**	**Mon 11/16/26**	**Wed 6/30/27**
Draft Feasibility Study Report Preparation	30 days	Mon 11/16/26	Fri 12/25/26
QA/QC Reviews	15 days	Mon 12/28/26	Fri 1/15/27
Feasibility Study Report Submitted to City	0 days	Fri 1/15/27	Fri 1/15/27
City Review of Feasibility Study Report	10 days	Mon 1/18/27	Fri 1/29/27
Final Feasibility Study Report Preparation	10 days	Mon 2/1/27	Fri 2/12/27
City Review / Meeting / Approval	98 days	Mon 2/15/27	Wed 6/30/27

EXHIBIT "C"

FEE PROPOSAL

S.O.W. Phase / Task	Total Hours	Labor Subtotal
Fully Burdened Labor Rates:		
Task 1 - Project Management & Administration		**$16,846**
1.1 Monthly Invoicing & Progress Reporting	14	$3,556
1.2 Coordination & Meetings	42	$9,408
1.3 Project Schedule	16	$3,882
Task 2 - Data Collection		**$17,756**
2.1 Record Data Collection & Review	54	$11,420
2.2 Aerial Survey Base Mapping	6	$1,584
2.3 Right of Way Base Mapping	6	$1,584
2.4 Utility Research and Base Mapping	12	$3,168
Task 3 - Conceptual Design		**$91,518**
3.1.1 General Plans & Foundation Plans	264	$53,868
3.1.2 Site Plans / Street Improvement Plans	10	$2,528
3.1.3 Stage Construction / Traffic Handling Plans	10	$2,528
3.2 Preliminary Cost Estimates	60	$12,310
3.3 Renderings	106	$20,284
Task 4 - Feasibility Study Report		**$19,912**
Feasibility Study Report Preparation	84	$19,912
	Labor Subtotal	**$146,032**
Subconsultants / Other Direct Costs (ODCs)	ODC: Mileage	$300
	ODC: Reproduction	$500
	Subconsultant: ERSC	$66,295
	Subconsultant/ODC Subtotal + 5% Markup	**$70,450**
	Total Fee	**$216,482**

EXHIBIT "D"

WORKERS' COMPENSATION INSURANCE CERTIFICATION

Every employer, except the State, shall secure the payment of compensation in one or more of the following ways:

(a) By being insured against liability to pay compensation by one or more insurers duly authorized to write compensation insurance in this State.

(b) By securing from the Director of Industrial Relations, a certificate of consent to self-insure, either as an individual employer, or as one employer in a group of employers, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his or her employees.

CHECK ONE

_____I am aware of the provisions of Section 3700 of the Labor Code which requires every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code, and I will comply with such provisions before commencing the performance of the work and activities required or permitted under this Agreement. (Labor Code §1861).

_____I affirm that at all times, in performing the work and activities required or permitted under this Agreement, I shall not employ any person in any manner such that I become subject to the workers' compensation laws of California. However, at any time, if I employ any person such that I become subject to the workers' compensation laws of California, immediately I shall provide the City with a certificate of consent to self-insure, or a certification of workers' compensation insurance.

I certify under penalty of perjury under the laws of the State of California that the information and representations made in this certificate are true and correct.

BIGGS CARDOSA ASSOCIATES, INC.

By:_____ Date: _____
Eric Pheifer, Principal/Vice President

COOPERATIVE AGREEMENT BETWEEN CITY OF REDLANDS AND REDLANDS UNIFIED SCHOOL DISTRICT FOR THE CITRUS AVENUE AND REDLANDS HIGH SCHOOL CROSSING PROJECT

This cooperative agreement ("Agreement") is made and entered in this 6th day of October, 2026 ("Effective Date"), by and between the City of Redlands, a municipal corporation (hereafter referred to as "City") and Redlands Unified School District, a school district organized and existing under the laws of the State of California, (hereafter referred to as "School District"). City and School District are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

RECITALS

WHEREAS, the City intends to complete a detailed conceptual design and cost estimate for the final design and construction of the Citrus Avenue and Redlands High School Crossing Project ("Project"); and

WHEREAS, the Project is located along Citrus Avenue between the north and south campuses of the Redlands High School; and

WHEREAS, the conceptual design cost of the Project is estimated to be two hundred sixteen thousand four hundred eighty-two dollars ($216,482); and

WHEREAS, the Project is identified in the City's Capital Project Need Analysis (CPNA) which will be funded through Measure I Arterial Programs; and

WHEREAS, the Measure I Arterial Programs will fund 76.9% of the Project costs, which is one hundred sixty-six thousand four hundred seventy-five dollars ($166,475), and the remaining 23.1% of the Project costs, which is fifty thousand seven dollars ($50,007), will be financed through the City's local fund; and

WHEREAS, the School District will share 50% of the City's cost of the project, which is twenty-five thousand three dollars and fifty cents ($25,003.50), as more particularly set forth in Attachment "A" which is attached hereto and incorporated herein by this reference; and

NOW THEREFORE, in consideration of the above recitals and the mutual covenants hereinafter contained, the Parties agree as follows:

SECTION 1
CITY'S OBLIGATIONS

City agrees to:

1. Act as Lead Agency in the execution of conceptual design services for the Project. As such, City shall be the sole Party that contracts with Consultant for conceptual design services.

2. Pay its share of the design costs if funding is reduced, relinquished, de-obligated, or otherwise no longer available.

3. Invoice School District for its share of conceptual design services costs no more frequently than once per month. Consultant invoices shall be included with invoices to City as the basis for substantiating the invoice amount for eligible design expenditures.

4. Establish and maintain an accounting conforming to Generally Accepted Accounting Principles to support accounting activities associated with the delivery of the design and produce monthly reports which clearly identify invoice payments for design services, including information on the funding sources.

SECTION II
SCHOOL DISTRICT'S OBLIGATIONS

School District agrees to:

1. Be responsible for the full conceptual design services costs of Project, totaling $25,003.50.

2. Pay its share of design costs if funding is reduced, relinquished, de-obligated, or otherwise no longer available.

3. Pay City for expenditures incurred for the project within thirty days following receipt of an invoice from City.

4. Establish and maintain an accounting conforming to Generally Accepted Accounting Principles to support accounting activities associated with the delivery of the design and produce monthly reports which clearly identify invoice payments for design services, including information of the funding sources.

SECTION III
MUTUAL OBLIGATIONS

1. That eligible Project expenditures shall be limited to conceptual design-specific work activities and shall not include escalation, interest, or other fees.

2. Each Party shall defend, indemnify, and hold harmless the other Party from and against any claim of liability, damages, cost or loss, including costs and attorney's fees, from personal injury or death to persons, or property damage (collectively "Claims") resulting from or arising from negligence or willful misconduct of either party, it's elected officials, employees, consultants, or agents, except to the extent such Claims may be caused by or result from negligence or willful misconduct of either party, it's elected officials, employees, contractors, or agents.

3. This Agreement shall commence on its Effective Date and shall terminate upon City's provision of a written notice of completion of design, unless any accounting remains

unsettled between the Parties. Upon settlement of any such accounting issues, City and School District shall each issue a written notice of completion of conceptual design and this Agreement shall be deemed terminated as of such date. This Agreement may be extended or terminated by mutual written consent of the Parties.

4. City and School District are authorized self-insured public entities for purposes of Professional Liability, Automobile Liability, General Liability and Worker's Compensation, and warrant that through their respective programs of self-insurance they have adequate coverage or resources to protect against liabilities arising out of City's and School District's performance of the terms, conditions, and obligations of this Agreement.

SECTION IV
INDEMNIFICATION

1. Indemnification by School District: School District shall indemnify, defend, and hold harmless City and its elected and appointed officials, officers, employees, agents, and volunteers from any and all claims, actions or losses, damages, and/or liability resulting from School District's negligent acts or omissions, or willful misconduct, which arise from School District's performance of its obligations under this Agreement.

2. Indemnification by City: City shall indemnify, defend, and hold harmless School District and its elected and appointed officials, officers, employees, agents and volunteers from any and all claims, actions, losses, damages and/or liability resulting from City's negligent acts or omissions, or willful misconduct, which arise from City's performance of its obligations under this Agreement.

3. Comparative Fault. In the event either Party is found to be comparatively at fault for any claim, action, loss or damage which results from their respective obligations under this Agreement, the Parties shall indemnify the other to the extent of its comparative fault.

SECTION V
ENFORCEMENT OF AGREEMENT

1. Governing Law: This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions. The Parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated only in the state courts located in San Bernardino County, California, and the federal courts located in Riverside County, California.

2. Attorneys' Fees: In the event any action is commenced to enforce or interpret this Agreement, the prevailing Party in any such action shall be entitled to its costs and reasonable attorneys' fees, including fees for use of in-house counsel by a Party.

3. Waiver: No waiver of any default shall constitute a waiver of any other default or breach, whether of the same or other covenant or condition. No waiver, benefit, privilege, or service voluntarily given or performed by a Party shall give the other Party any contractual

rights by custom, estoppel, or otherwise.

SECTION VI
MISCELLANEOUS PROVISIONS

1. Entire Agreement: This Agreement contains the entire agreement of the Parties with respect to subject matter hereof, and supersedes all prior negotiations, understandings or agreements regarding the same. No supplement, modification, or amendment of this Agreement shall be binding unless executed in writing and signed by both Parties.

2. Time of the Essence: Time is of the essence for each and every provision of this Agreement.

3. Interpretation: Because the Parties have participated fully in the preparation of this Agreement, the language of this Agreement shall be construed simply, according to its fair meaning, and not strictly for or against any Party. Any term referencing time, days, or period for performance shall be deemed Redlands work days. The captions of the various articles and sections are for convenience and ease or reference only, and do not define, limit, augment, or describe the scope, content, or intent of this Agreement.

4. Severability: If a court of competent jurisdiction declares any portion of this Agreement invalid, illegal, or otherwise unenforceable, the remaining provisions shall continue in full force and effect, unless the purpose of this Agreement is frustrated.

5. Incorporation: The Recitals are incorporated into the body of this Agreement.

6. Notice: Any notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a Party may provide notice in accordance with this section:

To the City:	City Clerk City of Redlands 35 Cajon Street P.O. Box 3005 (Mailing) Redlands, CA 92373 Email: jdonaldson@cityofredlands.org Phone: (909) 798-7531
To School District:	Redlands Unified School District 20 W. Lugonia Avenue

Redlands, CA 92374
Attn: Superintendent of Schools

7. Laws and Regulations: The Parties shall keep themselves fully informed of and in compliance with all local, state and federal laws, rules and regulations in any manner affecting the Parties' performance of this Agreement. A Party shall not be liable for the other Party's violation of any laws or regulations in connection with this Agreement. If a Party identifies any conflict or possible conflict between its obligations hereunder and applicable laws, rules and regulations, that Party shall provide immediate written notice to the other Party.

8. Assignment: This Agreement is not assignable by either Party, in whole or in part, without the consent of the other Party in the form of a formal written amendment. Any assignment or attempted assignment without such consent may, in the sole discretion of the non-assigning Party, result in the immediate termination of this Agreement.

9. Independent Contractor: The Parties agree and intend that each Party be deemed an independent entity, and do not create by this Agreement any partnership, joint venture, or similar business arrangement, relationship, or association between them, except as may be agreed to expressly by this Agreement. Each Party shall perform their services hereunder in an independent capacity and not as an employee or agent of the other Party.

----- SIGNATURES ON THE FOLLOWING PAGE -----

IN WITNESS WHEREOF, duly authorized representatives of City and School District have signed this Agreement.

REDLANDS UNIFIED SCHOOL DISTRICT

By:_____
Juan J. Cabral
Superintendent

Date:_____

ATTEST:

By:_____
Clerk of the Board

CITY OF REDLANDS

By:_____
Mario Saucedo
Mayor

Date:_____

APPROVED AS TO FORM:

By:_____
Yvette M. Abich Garcia
City Attorney

ATTEST:

By:_____
Jeanne Donaldson
City Clerk

Attachment A

Project Scope:

The Project will evaluate, develop, and conceptual design a pedestrian crossing improvement along Citrus Avenue between the north and south campuses of Redlands High School.

Conceptual Design Cost and Funding Shares:

Measure I Arterial Fund: 76.9%
City Development Share: 23.1% (50-50 split between City and School District)

			LOCAL DEVELOPMENT SHARE	
PHASE	**TOTAL COST**	**MEASURE I**	**CITY**	**SCHOOL DISTRICT**
Conceptual Design	$216,482	$166,475	$25,003.50	$25,003.50
TOTAL	**$216,482**	**$166,475**	**$25,003.50**	**$25,003.50**

City Council **AGENDA ITEM NO. I14.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve the Interlocal Agreement between the Town of Apple Valley and the Cities of Adelanto, Barstow, Chino, Colton, Fontana, Hesperia, Highland, Montclair, Ontario, Rancho Cucamonga, Redlands, Rialto, San Bernardino, Upland, Victorville, Yucaipa and San Bernardino County for the 2025 Justice Assistance Grant Award and approve an additional appropriation of $16,248 to the Redlands Police Department (Police Chief Tolber)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

I move to approve the Interlocal Agreement between the Town of Apple Valley and the Cities of Adelanto, Barstow, Chino, Colton, Fontana, Hesperia, Highland, Montclair, Ontario, Rancho Cucamonga, Redlands, Rialto, San Bernardino, Upland, Victorville, Yucaipa and San Bernardino County for the 2025 Justice Assistance Grant Award and approve an additional appropriation of $16,248 to the Redlands Police Department.

RECOMMENDATION:

Staff recommends that the City Council approve the Interlocal Agreement between the Town of Apple Valley and the Cities of Adelanto, Barstow, Chino, Colton, Fontana, Hesperia, Highland, Montclair, Ontario, Rancho Cucamonga, Redlands, Rialto, San Bernardino, Upland, Victorville, Yucaipa and San Bernardino County for the 2025 Justice Assistance Grant Award and approve an additional appropriation of $16,248 to the Redlands Police Department.

DISCUSSION:

As in past years, the Redlands Police Department (RPD) is entitled to a share of the Justice Assistance Grant (JAG) Award funds, which are allocated based on city population. All of the above-listed governmental agencies agree to allow the County of San Bernardino to administer the grant funds and distribute each agency’s allocated share for expenditure in accordance with JAG guidelines.

RPD's approved proposal seeks to purchase rifle-rated ballistic shields. These shields are designed to provide protection against high-velocity rifle rounds during critical incidents, including active shooter situations, high-risk warrant service, and other violent encounters. Currently, many standard-issue ballistic shields are rated only for handgun threats, which limits officer safety when confronting increasingly common rifle-equipped suspects. The acquisition of rifle-rated shields will allow officers to safely approach, contain, and resolve high-risk situations while minimizing exposure to life-threatening injuries. Ultimately, this project supports the broader goal of strengthening community safety and ensuring that officers are adequately protected while serving the public.

ALTERNATIVES:

The City Council may elect not to approve the Interlocal Agreement and accept the the grant funds.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Rachel Tolber, Police Chief

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jimmy Nguyen, Management Analyst

FISCAL IMPACT

Fiscal Year:

Revenue Generating: No

Amount: $16,248

Budgeted Y/N:

Account No.: 200202

Additional Appropriation Required: Yes

Discussion:

There is no impact to the General Fund because all expenditures are reimbursable under the grant.

Attachments

Additional_Appropriation_Form_FY25_JAG.pdf
JAG_2025_Award_-_Interlocal_Agreement.pdf

CITY OF REDLANDS
REQUEST FOR ADDITIONAL APPROPRIATION

DATE OF REQUEST: 10/06/2026

FINANCE USE ONLY
TRANSACTION NO:
ACCOUNTING PERIOD:

An additional appropriation is hereby requested as follows:

Department: Police

EXPENDITURE APPROPRIATION INCREASE (if applicable)				
Account Description	**Orgkey**	**Object Code**	**Job Ledger (If applicable)**	**Amount**
Special Departmental Supplies	200202	7810	TBD	16,248.00
			TBD	
			TBD	
				$ 16,248.00 -

REVENUE APPROPRIATION INCREASE (if applicable)				
Account Description	**Orgkey**	**Object Code**	**Job Ledger (If applicable)**	**Amount**
Federal Grants	200202	4407	TBD	16,248.00
				$ 16,248.00 -

JUSTIFICATION: FY25 JAG Grant

Requested By: Rachel Tolber
Department Head

Recommended By Finance Director:

Yes _____ No _____ Signed _____

Recommended: _____
City Manager

Comments: _____

Approved by City Council:

Date: _____

Signed: _____
City Clerk

INTERLOCAL AGREEMENT
BETWEEN THE TOWN OF APPLE VALLEY AND THE CITIES OF ADELANTO, BARSTOW, CHINO, COLTON, FONTANA, HESPERIA, HIGHLAND, MONTCLAIR, ONTARIO, RANCHO CUCAMONGA, REDLANDS, RIALTO, SAN BERNARDINO, UPLAND, VICTORVILLE, YUCAIPA, AND SAN BERNARDINO COUNTY, CA

CONCERNING DISTRIBUTION OF THE
2025 JUSTICE ASSISTANCE GRANT AWARD

This Agreement is made and entered into this 1 day of September, 2026, by and between SAN BERNARDINO COUNTY, acting by and through its governing body, the Board of Supervisors (hereinafter referred to as "COUNTY"), and the aforementioned TOWNS (hereinafter referred to as "TOWNS") and named CITIES (hereinafter referred to as "CITIES"), acting by and through their respective governing bodies, the Town Councils and City Councils, all of whom are situated within San Bernardino County, State of California, as follows:

WHEREAS, each governing body, in performing governmental functions or in paying for the performance of governmental functions hereunder, shall make that performance or those payments from current revenues legally available to that party; and

WHEREAS, each governing body finds that the performance of this Agreement is in the best interests of all parties, that the undertaking will benefit the public, and that the division of costs fairly compensates the performing party for the services or functions under this Agreement; and

WHEREAS, the TOWNS and CITIES acknowledge that under this Agreement they shall request reimbursement from COUNTY only for eligible expenditures that are properly documented and consistent with allowable JAG activities under the FY25 JAG guidelines and applicable federal guidelines, including 2 CFR Part 200 and Bureau of Justice Assistance (BJA) special conditions; and COUNTY agrees to reimburse TOWNS and CITIES for their respective grant allocations as reflected in Appendix 1, less five percent (5%) retained by COUNTY for administrative costs related to oversight and management of subawards, and TOWNS and CITIES acknowledge that the five percent (5%) administrative fee will be used by COUNTY to administer their programs during the permissible period of performance; and

WHEREAS, the TOWNS and CITIES agree that all JAG funds will be distributed and reimbursed in accordance with this Agreement and applicable FY25 JAG requirements.

WHEREAS, TOWNS and CITIES agree that they will enter into subrecipient agreements with COUNTY after the federal JAG award is received.

NOW THEREFORE, the COUNTY and TOWNS and CITIES agree as follows:

Section 1. Reimbursement of Funds

COUNTY shall reimburse TOWNS and CITIES for eligible expenditures incurred in connection with the FY25 JAG Award upon submission of proper documentation and verification that such costs comply with applicable federal requirements, including 2 CFR Part 200, and FY25 JAG guidelines. COUNTY shall retain five percent (5%) of the total JAG award for administrative purposes related to the management of subawards and compliance monitoring, as reflected in

Appendix 1. No funds shall be advanced prior to documented expenditures, and all reimbursement requests shall be subject to review and approval by COUNTY prior to payment.

Section 2. Fund Management and Allowable Expenditures

TOWNS and CITIES shall ensure that all expenditures submitted for reimbursement are consistent with allowable JAG uses and properly documented in accordance with federal regulations and the FY25 JAG requirements. When applicable, no expenditure shall be deemed eligible for reimbursement until the TOWN or CITY has completed all required federal certifications for its planned JAG-funded activity. These certifications may include, but are not limited to, the Certifications and Assurances by the Chief Executive of the Applicant Government, the Body-Worn Camera Policy Certification when body-worn camera expenditures are planned, the Body Armor Mandatory Wear Policy Certification when body armor is purchased, the Extreme Risk Protection Order Certification when ERPO-related activities are funded, the Unmanned Aircraft System (UAS) or Counter-UAS Certification when applicable, and any required documentation for the purchase of items otherwise prohibited without federal waiver. COUNTY shall not process reimbursements for any jurisdiction until all applicable certifications are provided.

TOWNS and CITIES acknowledge responsibility for compliance with all applicable federal regulations, including civil rights, anti-discrimination, and any special conditions imposed by the Bureau of Justice Assistance.

Section 3. Subrecipient Agreement

TOWNS and CITIES shall execute subrecipient agreements with COUNTY prior to commencing project activities under this Agreement or submitting any reimbursement requests under the FY25 JAG Award. These agreements shall include acknowledgment of the federal award, compliance with all applicable special conditions, responsibility for maintaining records, timely submission of programmatic and financial reports, and consent to monitoring or audit by COUNTY or federal authorities. Eligible costs incurred during the allowable period of performance may be reimbursed, provided such costs are allowable, properly documented, and incurred in compliance with applicable federal requirements and FY25 JAG guidelines. TOWNS and CITIES acknowledge that reimbursement is contingent upon full execution of the subrecipient agreement and compliance with its terms and applicable federal regulations.

Section 4. Reporting and Compliance

TOWNS and CITIES agree to provide COUNTY with any information or documentation requested to comply with federal reporting, monitoring, and audit requirements within five (5) business days of request. This includes supporting documentation for all expenditures submitted for reimbursement and performance measurement data.

Section 5. Liability

Nothing in this Agreement shall impose liability on COUNTY, TOWNS, or CITIES beyond that authorized by law. Each party is responsible for its own actions and shall not be liable for claims arising from another party's expenditures, reimbursement requests, or use of JAG funds.

Section 6. No Third-Party Rights

The parties to this Agreement do not intend for any third party to obtain a right by virtue of this Agreement.

Section 7.

This Agreement does not create any obligations beyond those expressly set forth herein. TOWNS, CITIES, and COUNTY shall comply with all applicable federal and state laws governing the use of federal funds, including the FY25 JAG requirements, and any regulations issued by the Bureau of Justice Assistance or the Office of Justice Programs. Reimbursement shall be the sole method of disbursing JAG funds under this Agreement.

Section 8.

This Agreement shall be effective from October 1, 2024 and shall continue through September 30, 2028, unless amended by mutual agreement of all parties.

Section 9.

This Agreement shall be governed by the laws of the State of California. The parties agree that the venue of any action or claim brought by any party to this Agreement will be the Superior Court of California, County of San Bernardino, San Bernardino District.

Section 10.

The parties are authorized self-insured or partially self-insured public entities for purposes of Professional Liability, General Liability, Automobile Liability and Worker's Compensation and warrant that through their respective programs of self-insurance and insurance, they have adequate coverage or resources to protect against liabilities arising out of performance of the terms, conditions or obligations of this Agreement.

Section 11.

This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other mail transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request

WHEREFORE, all parties freely and voluntarily agree to all of the above terms.

SAN BERNARDINO COUNTY

_____
Dawn Rowe, Chair, County Board of Supervisors

Dated: _____
SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
San Bernardino County

By_____
Deputy

APPROVED AS TO FORM:

_____
*Daniella V. Hernandez, Deputy
County Counsel

*By law, the County Counsel's Office may only advise or approve contracts or legal documents on behalf of its clients. It may not advise or approve a contract or legal document on behalf of other parties. Our view of this document was conducted solely from the legal perspective of our clients. Our approval of this document was offered solely for the benefit of our clients. Other parties should not rely on this approval and should seek review and approval by their own respective attorneys.

TOWN OF APPLE VALLEY, CA

_____
Town Manager

ATTEST:

_____
Town Clerk

APPROVED AS TO FORM:

_____
Town Attorney

/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF ADELANTO, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF BARSTOW, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF CHINO, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF COLTON, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF FONTANA, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF HESPERIA, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF HIGHLAND, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF MONTCLAIR, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF ONTARIO, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF RANCHO CUCAMONGA, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF REDLANDS, CA

_____
Mayor

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF RIALTO, CA

_____
City Administrator

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF SAN BERNARDINO, CA

_____
Mayor

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF UPLAND, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF VICTORVILLE, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

CITY OF YUCAIPA, CA

_____
City Manager

ATTEST:

_____
City Clerk

APPROVED AS TO FORM:

_____
City Attorney
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

JAG 2025 Allocations

Jurisdiction	Allocation	5% Admin Fee	Award
San Bernardino County	$ 139,611	$ (6,981)	$ 132,630
Adelanto	$ 21,445	$ (1,072)	$ 20,373
Apple Valley	$ 28,762	$ (1,438)	$ 27,324
Barstow	$ 18,399	$ (920)	$ 17,479
Chino	$ 22,357	$ (1,118)	$ 21,239
Colton	$ 16,216	$ (811)	$ 15,405
Fontana	$ 45,601	$ (2,280)	$ 43,321
Hesperia	$ 38,861	$ (1,943)	$ 36,918
Highland	$ 27,754	$ (1,388)	$ 26,366
Montclair	$ 18,975	$ (949)	$ 18,026
Ontario	$ 45,169	$ (2,258)	$ 42,911
Rancho Cucamonga	$ 40,828	$ (2,041)	$ 38,787
Redlands	$ 17,103	$ (855)	$ 16,248
Rialto	$ 38,381	$ (1,919)	$ 36,462
San Bernardino	$ 192,480	$ (9,624)	$ 182,856
Upland	$ 17,415	$ (871)	$ 16,544
Victorville	$ 80,648	$ (4,032)	76,616
Yucaipa	$ 13,025	$ (651)	$ 12,374
~~Yucca Valley~~	~~$ -~~	~~$ -~~	~~$ -~~
Total	**$ 823,030**	**$ (41,151)**	**$ 781,879**

$ 132,630	county alloc.	
$ 41,151	admin alloc.	$ 82,284 Sheriff
$ 649,249	city alloc.	$ 50,346 DA
$ 823,030		**$ 132,630**

* Yucca Valley opt-out

City Council **AGENDA ITEM NO. I15.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve the use of City resources and an in-kind request in the amount of $5,798.32 related to A Holiday Evening with Phat Cat Swinger event held on Friday, December 4, 2026, hosted by Redlands Bowl Performing Arts; approve various temporary street closures; and determine that the event is categorically exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's guidelines implementing the California Environmental Quality Act; and

2. I move to approve in-kind support in the amount of $5,798.32, and the temporary street closures related to A Holiday Evening with Phat Cat Swinger event to be held on Friday, December 4, 2026.

RECOMMENDATION:

Staff recommends that the City Council approve the request for in-kind support in the amount of $5,798.32 for Redlands Bowl Performing Arts A Holiday Evening with Phat Cat Swinger event to be held on Friday, December 4, 2026, and approve the temporary street closures. Staff further recommends that the City Council determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act.

DISCUSSION:

The Facilities and Community Services Department manages the administration and issuance of permits for special events held in public areas of the City. Upon the issuance of a special event permit, the event may take place contingent on the event organizer paying the required fees. The City recognizes the value of partnering with non-profit agencies and organizations to provide beneficial services to the community. In an effort to support programs that provide community benefit, the City Council will, from time to time, consider the authorization of in-kind support, including the use of City equipment, staff and facilities for special events.

The Redlands Bowl Performing Arts is preparing to host A Holiday Evening with Phat Cat Swinger event, scheduled to take place on Friday, December 4, 2026, at 7:00 p.m. at the Redlands Bowl. According to the applicant, the event is anticipated to attract over 6,000 attendees. Redlands Bowl Performing Arts envisions this year's holiday celebration as a community-centered gathering that strengthens the City since the attendees will shop and dine throughout the City before and after the program.

Redlands Bowl Performing Arts is requesting in-kind support valued at an estimated $5,798.32, including Police, Fire, and Facilities and Community Services personnel and equipment. Previously in 2025, the City Council approved $5,860.00 in in-kind support for a similar event hosted on Friday, December 12, 2025, called Christmas under the Stars.

In addition, Redlands Bowl Performing Arts is requesting temporary street closures of Grant Street between West Olive Avenue and Brookside Avenue; Eureka Street between West Olive Avenue and Brookside Avenue; and West Vine Street between Eureka Street and Cajon Street from 4:00 p.m. to 10:00 p.m. on Friday, December 4, 2026.

This event qualifies for a categorical exemption from CEQA review under Section 15311(c) of the CEQA Guidelines, which applies to temporary or minor use of land having negligible or no permanent effects, including temporary placement of mobile food units, portable restrooms, or similar facilities in public parks or other facilities designed for public use.

ALTERNATIVES:

The City Council may elect to deny the request for in-kind support, deny the request for temporary street closure and direct staff accordingly.

STRATEGIC PLAN:

Priority A - Quality of Life, Beautification, Arts and Culture.

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jaclyn Ramirez, Administrative Assistant

FISCAL IMPACT

Fiscal Year: 2026/27

Revenue Generating: No

Amount: $5,798.32

Budgeted Y/N: No

Account No.: N/A

Additional Appropriation Required: No

Discussion:

Please see the "Fiscal Impact" attachment for reference.

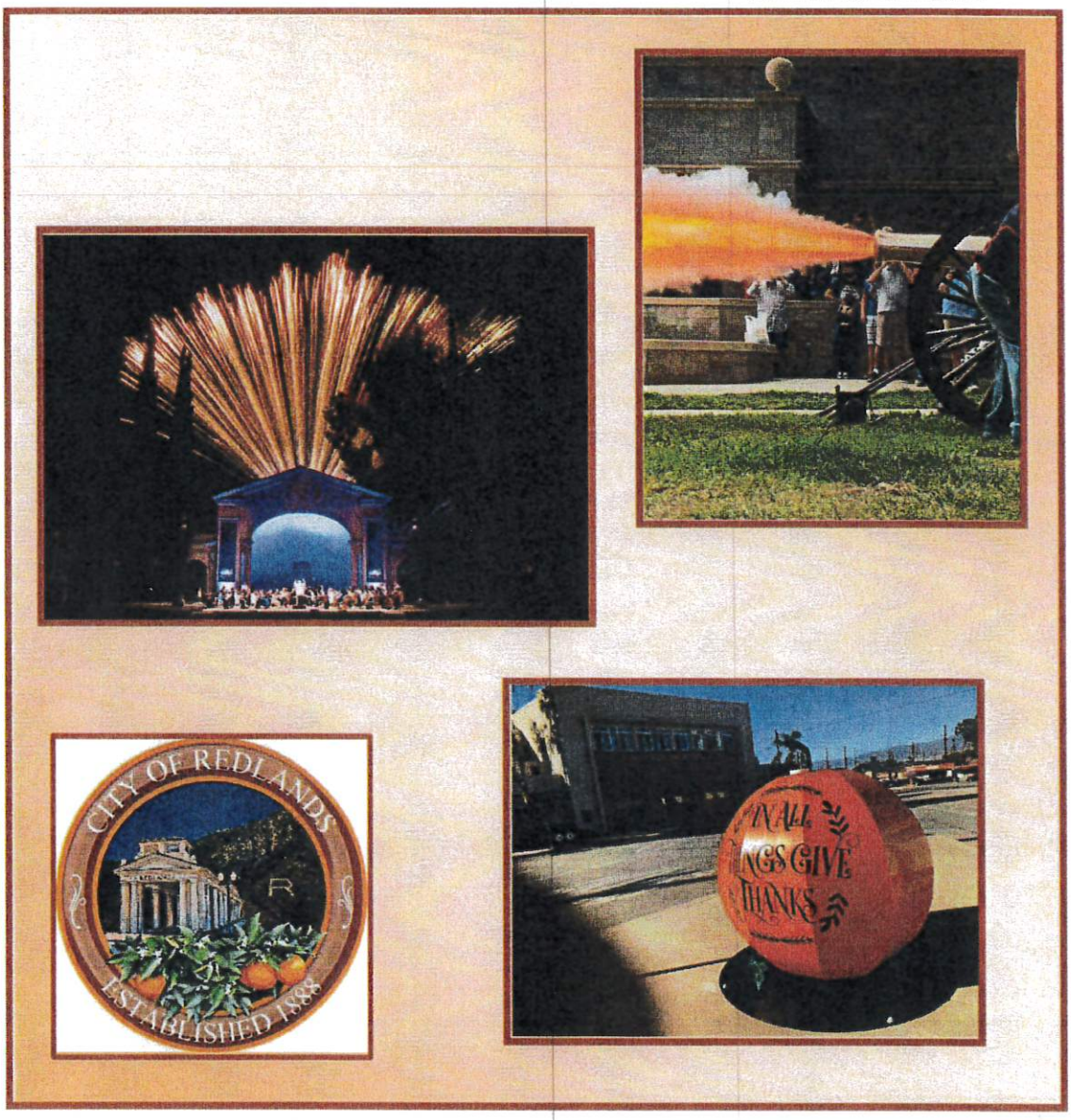
Attachments

A_Special_Event_Application_-_Holiday_Evening_w_Phat_Cat_Swinger.pdf
B_In-Kind_Request_-_Holiday_Evening_w_Phat_Cat_Swinger.pdf
C_Verification_of_Non-Profit_-_Holiday_Evening_w_Phat_Cat_Swinger.pdf
D_Street_Closure_Permit_-_Holiday_Evening_w_Phat_Cat_Swinger.pdf
E_RCMA_Closure_Map.pdf
F_Fiscal_Impact_-_Holiday_Evening_w_Fat_Cat_Swinger.pdf

City of Redlands
35 Cajon Street, Ste. 222
Redlands, CA 92373
(909) 798-7655 ext 3

SPECIAL EVENTS PERMIT APPLICATION

EVENT: Holiday Evening with Phat Cat Swinger
ORGANIZER: Redlands Bowl Performing Arts
Date of Event: 12 / 4 / 26
Date Submitted: 4 / 22 / 26



NOTICE TO PERMIT APPLICANT

- Completed Special Event Permit Applications **must** be submitted to the Facilities & Community Services Department a **minimum of four (4) months prior** to the date the event is scheduled to begin.
- All forms in this application package that are relevant to your event must be complete and submitted together in order to be considered.
- Applicants must conform to all requirements for maintaining liability insurance.
- Incomplete applications or applications submitted past the deadline are subject to denial of request to hold event.

SUMMARY OF EVENT

Event Title A Holiday Evening with Phat Cat Swinger

Description Holiday Christmas Concert

Date/Time

Setup	Date	12/4/26	Time	4:30pm	Location(s)	Redlands Bowl
Event Starts	Date	12/4/26	Time	7:00pm	Location(s)	Redlands Bowl
Event Ends	Date	12/4/26	Time	9:00pm	Location(s)	Redlands Bowl
Dismantle	Date		Time		Location(s)	

*Submit a Site Plan for each venue listed

Anticipated Attendance: Total 6,000 Per Day 6,000

Anticipated Participants: Total 6,500 Per Day 6,000

CONTACTS Person(s) or Agent(s) responsible for and authorized to represent this event on all matters:

	Primary Contact:	Secondary Contact
Name:	Beverly Noerr	Valerie Peister
Address:	168 S. Eureka St.	168 S. Eureka St.
City, State, Zip	Redlands, CA 92373	Redlands, CA 92373
Phone:	(909) 793-7316	(909) 793-7316
Email:	bnoerr@redlandsbowl.org	vpeister@redlandsbowl.org

Name of Organization: Redlands Bowl Performing Arts Is it Non-Profit? ✓
Tax I.D. #:

Yes	No	
✓		Is this an annual event? How many years have you been holding this event? 2
✓		Street Closure(s) requested? If yes, please complete Street Closure Permit Application and Barricade Rental Form in Appendix A
	✓	Does this event involve a parade? Please complete Parade/Public Assemblies Permit Application form in Appendix A
	✓	Will you be serving alcohol? If yes, please complete both Alcohol Permit forms in Appendix A
	✓	Are you requesting use of the Prospect Park Sign? If yes, please complete the Sign Request form in Appendix A
	✓	Are you requesting use of the City Stage? If yes, please complete the Show Mobile Rental form in Appendix A
✓		Vendor(s)? If yes please complete the Vendor List in Appendix A.

SITE PLAN

Your event site plan/route map should include but not be limited to:

- ☑ An outline of the entire event venue including the names of all streets or areas that are part of the venue and the surrounding area. If the event involves a moving route of any kind, indicate the direction of travel and all street or lane closures.
- ☑ The location of fencing, barriers and/or barricades. Indicate any removable fencing for emergency access.
- ☑ The provision of minimum twenty foot (20') emergency access lanes throughout the event venue.
- ☑ The location of first aid facilities and ambulances.
- ☑ The location of all stages, platforms, scaffolding, bleachers, grandstands, canopies, tents, portable toilets, booths, beer gardens, cooking areas, trash containers and dumpsters, and other temporary structures.
- ☑ A detail or close-up of the food booth and cooking area configuration including booth identification of all vendors cooking with flammable gases or barbecue grills
- ☑ Generator locations and/or source of electricity.
- ☑ Placement of vehicles and/or trailers.
- ☑ Exit locations for outdoor events that are fenced and/or locations within tents and tent structures.
- ☑ Identification of all event components that meet accessibility standards.
- ☑ A parking and/or shuttle plan for events that are likely to exceed parking lot capacity of the space you are using.
- ☑ Other related event components not listed above.

TIMELINE

Please provide a narrative and timeline of your event. You may provide this information as an attachment if necessary.

HOUR	ACTION
4:00 pm	Joslyn Senior Center Parking Closed
5:00pm	Eureka and Grant Closure
5:00pm to 6:30 pm	Handicap and Artist parking
7:00 pm	Event Introduction / Begins
8:30 pm	Intermission
9:00 pm	Event Ends

MARKETING AND PUBLIC RELATIONS

Yes No

☑ ☐ Will this event be marketed, promoted, or advertised in anymanner?

f yes, please describe Banners, flyers, social media

☐ ☑ Will there by live media coverage during the event?

f yes, please describe _____

☐ ☑ Will media vehicles be parked within the event venue?

f yes, please describe safety plan _____

☐ ☑ Do you have a plan to control or limit the placement and/or distribution of promotional signage, stickers, and other items?

f yes, please describe _____

INSURANCE REQUIREMENTS

Regardless of the event you are required to have insurance that indemnifies the city of Redlands listing the location date and time.

Name of Insurance Agency HUB International Insurance Services, Inc

Address Street 3390 University Ave. Ste. 300

City Riverside State CA Zip 92501

Telephone Day 909-379-1332 Evening _____ Fax _____ Pager/Cellular _____

Contact Name Kim Katz

Policy Type Commercial Umbrella

Policy Amount $3,000,000

Policy Number 01-UB-0013982-01-13

SECURITY PLAN

YES NO

☐ ☑ Have you hired a licensed professional security company to develop and manage your event's security plan? If yes, you are required to provide a copy of the security company's valid Private Patrol Operator's License issued by the State of California.

Security Organization RPD - 2 Officers

Address Street _____

City _____ State _____ Zip _____

Telephone Day _____ Evening _____ Fax _____ Pager/Cellular _____

Private Patrol Operator License# _____

Please describe your security plan including crowd control, internal security or venue safety, or attach the plan to this application. Event typically has (2) officers on standby walking the premisis.

MEDICAL PLAN

Any event that has physical activity or is a race and has above 50 people requires amedical plan.

YES NO

☐ ☑ Have you hired a licensed professional emergency medical services provider to develop and manage your event's medical plan?

If yes, please list:

Medical Services Provider Redlands Fire Department

Address Street 35 Cajon St., Ste. 12

City Redlands State CA Zip 92373

Telephone Day (909)307-7313 Evening _____ Fax _____ Pager/Cellular _____

Please describe your medical plan including your communications plan, the number, certification levels (MD, RN, Paramedic, EMT) and types of resources that will be at your event and the manner in which they will be managed and deployed. Your plan should include hours of setup and dismantle of medical aid areas. You may attach the plan to this application if necessary.

We have a dedicated booth to handle medical emergencies.

ACCESSIBILITY PLAN

This checklist is intended to serve as a planning guideline and may not be inclusive of all City, County, State and Federal access requirements. You may attach more detailed information if necessary.

YES NO

☑ ☐ Will there be a Clear Path of Travel throughout your event venue? Please describe Well lit areas to gain access to exits and plenty of paths.

☑ ☐ Have you developed a Disabled Parking and/or Transportation Plan (including the use of public transportation or shuttle services) for your event? Please describe The use of Smiley library parking and Eureka St. helps those guests

☑ ☐ Will a minimum of 10% of portable rest rooms at your event be accessible? Please describe They have restrooms attached to Mission Gables.

☑ ☐ Will all food, beverage and vending areas be accessible? Please describe Yes, ~~[illegible]~~ Optimist will sell at their booth at back of venue.

☑ ☐ Will all signage be provided in highly contrasting colors and placed so pedestrian flow will not obstruct its visibility? Please describe Staff will also be around to help guide guests

☐ ☑ If telephones are provided, will at least one telephone at each phone bank have a volume control and is hearing aid compatible? Please describe

☑ ☐ If an information center is provided at your event will customer service representatives be available to assist disabled individuals? Please describe There will be (1) booth at each entrance to assits guests.

☑ ☐ If all areas of your event venue cannot be made accessible will maps or programs be made available to show the location of accessible rest rooms, parking, phones (if any), drinking fountains, and first aid stations? Please describe

RESTROOM FACILITIES PLAN

You are required to provide portable rest room facilities at your event, unless you can substantiate the sufficient availability of both ADA accessible and non-accessible facilities in the immediate area of the event site which will be available to the public during your event. Indicate on your timeline when portable toilets will be set up.

Yes No

☐ ☑ Do you plan to provide portable rest room facilities at your event?

If yes: Total number of portable toilets

If no: Please explain: Permenant facilities on site.

Rest Room Company

Address Street

City State Zip

Telephone Day Evening Fax Pager/Cellular

LIST OF VENDORS

Please provide a list of vendors, what they are there for and their business license numbers. Keep in mind that this list of vendors cannot change after the event has been approved. All must have a Redlands business license in order to participate with your event. If you need more entries, please attach a list with the same information to your event package. Vendors include all businesses either performing a service or selling at your event. All food concessioners must meet the San Bernardino Counties Department of Public Health Food Handler's and Fire Suppression requirements.

Yes No

- ☐ ☑ Will items or services be sold at your event?
- ☑ ☐ Will you have some education only (not selling a product or service) booths?
- ☐ ☑ Will items or services sold at your event present unique liability issues (e.g. massage, etc.)?
- ☑ ☐ Does your event include food concession and/or preparation areas?
- ☑ ☐ Do you intend to cook food in the event area?

If yes, please specify method:

- ☐ Gas
- ☑ Electric
- ☐ Charcoal
- ☐ Other (specify) _____

VENDOR	SERVICE THEY ARE PROVIDING	REDLANDS BUSINESS LICENSE NUMBER	EDUCATIONAL INFORMATION ONLY? (Y/N)
Optimist Club	Concessions		

ENTERTAINMENT PLAN

YES NO

☑ ☐ Are there any musical entertainment features related to your event?

If yes, complete the following information or provide an attachment listing all bands/performers, type of music, sound check and performance schedule.

Number of Stages 1

Number of Performers/Bands 1

Performer/Band name and music type Phat Cat Swinger

☑ ☐ Will sound checks be conducted prior to the event?

If yes, Start time 5:00 pm Finish time 6:00 pm

☑ ☐ Will sound amplification be used?

If yes, Start time 5:00 pm Finish time 9:00pm

☑ ☐ Do you plan to have a patron dance component to either live or recorded music at your event?

If yes, please describe at times, the audience will dance up front

☑ ☐ Please describe the sound equipment that will be used for your event Redlands Bowl Sound Equipment

☐ ☑ Will inflatables, such as jumpers, or similar devices be used at your event?

If yes, please describe

☐ ☑ Does your event include the use of fireworks, rockets, lasers, or other pyrotechnics?

If yes, please fill out a fireworks permit also located in this packet.

If yes, please describe

☑ ☐ Will your event include the use of any signs, banners, decorations, or special lighting?

If yes, please describe Yes, all marketing content

☐ ☑ Will there be massage activities at your event? If yes, please describe

☐ ☑ Do your event plans include any, drawings or raffle opportunities?

If yes, please describe

ALCOHOL

Please Note: You will need to have your alcohol permit approved by Redlands city council prior to your event. A copy of your Alcohol license will be needed after city council approval, before the event.

Yes No

☐ ☑ Does your event involve the use of alcoholic beverages?

If yes, please check all that apply:

- ☐ Free/Host Alcohol
- ☐ Alcohol Sales
- ☐ Host and Sale Alcohol
- ☐ Beer
- ☐ Beer and Wine
- ☐ Beer, Wine and Distilled Spirits

Please describe your security plan to ensure the safe sale or distribution of alcohol at your event. _____

MITIGATION OF IMPACT

YES NO

☑ ☐ Have you met with the residents, businesses, places of worship, schools and other entities that may be directly impacted by your event? If yes, please attach a complete list of these entities.

If no, please explain emails to surranding businesses and places of worship.

☐ ☐ Do you have a sample of the notice that you propose to distribute two weeks prior to your event? If yes, please attach.

If no, please explain _____

AFFIDAVIT OF APPLICANT

I certify that the information contained in the foregoing application is true and correct to the best of my knowledge and belief that I have read, understand and agree to abide by the rules and regulations governing the proposed Special Event under the Redlands Municipal Code and I understand that this application is made subject to the rules and regulations established by the City Council and/or the City Manager or the City Manager's designee. Applicant agrees to comply will all other requirements of the City, County, State, Federal Government, and any other applicable entity which may pertain to the use of the Event venue and the conduct of the Event. In the event that a possessory interest subject to property taxation is created by virtue of this use permit, I agree to pay all possessory interest taxes and the City shall not be liable for the payment of such taxes I further agree that the payment of any such taxes shall not reduce any consideration paid to the City pursuant to this use permit. I agree to abide by these rules, and further certify that I, on behalf of the Host Organization, am also authorized to commit that organization, and therefore agree to be financially responsible for any costs and fees that may be incurred by or on behalf of the Event to the City of Redlands.

Print Name of Applicant/Host Organization Redlands Bowl Performing Arts

Title Executive Director

Signature

Date 4/22/2026

Print Name of Professional Event Organizer

Title Same -

Signature

Date

City of Redlands

In-Kind Support Request

Event Name: A Holiday Evening with Phat Cat Swinger

Event Date(s): 12/4/26 **Location(s):** 25 Grant St.

Rain Out Date: N/A **Beginning Time:** 7:00 pm **End Time:** 9:00 pm

Describe Your Request:

This completed form with all supporting documentation shall be submitted a minimum of 60 days prior to the scheduled event. Additional information may be attached to this application form, as needed.

Requesting RPD Presence/street closure

Select and Describe All City Provided Services That May Apply to Your Request :

- [x] Traffic (*Personnel, equipment, cones, barricades, no-parking* Barricades and street closure
- [x] Police (*Public Safety Personnel)* 2 officers
- [x] Fire (*Paramedics, Inspectors)*
- [x] Parks *(Cleanup Personnel, Ball Field Lights)*
- [x] Facility Redlands Bowl

Refuse/Recycling *(Event Receptacles, Roll-Off Service)* acquired by Event Organizers through Redlands Customer Service

Section 13.65 of the Redlands Municipal Code requires that events that serve more than 2,000 individuals per day will be required to submit for review and approval a Large Venue Recycling Plan. The Quality of Life Department may require smaller events to comply with City recycling practices as a condition of waiving fees.

- [x] Other FCS staff, maintaing Parks / Trash

Group/Organization Name: Redlands Bowl Performing Arts

Is your Group/Organization a Registered Non-Profit: [x] Yes [ ] No **Non-Profit Federal Tax ID Number:**

Does your Group/Organization Presently Have Liability Insurance? [■] Yes [ ] No

Please be advised that depending upon your request, you may be required to provide proof of insurance coverage in an amount determined by the City and naming the City as an additional insured.

Has your Group/Organization received fee waivers from the City in the past? Yes

Primary Contact Name & Title: Beverly Noerr, Executive Director

Mailing Address: 168 S. Eureka St

Phone Number: (909) 793-7316 **E-Mail Address:** bnoerr@redlandsbowl.org

As a part of our commitment to fiscal responsibility, the City of Redlands gathers data associated with the economic and social benefits associated with in-kind support. Please provide estimates, as applicable, for your event.

Positive outcomes for your organization from this

Attendees shop and dine throughout the city before and after the program. We continue to receive calls from patrons asking the steps to provide saftey for guests at the Bowl.

Describe what economic benefit and impact this event will bring to the City:

By providing officers, the public will feel safer and continue to attend, as well as shop and dine in redlands.

In April 2002, the City Council adopted Resolution No. 6038, which encourages groups or organizations requesting in-kind support from the City to use local businesses when procuring goods and services associated with the event. Receipts will need to be submitted through a follow up form. Failure to submit post event documentation (within 15 days) may affect future requests.

	Proposed Event	Previous Event Actuals	Vendors
Attendance: Redlands Residents	5,000	5,000	
Attendance: Non-Residents	1,000	1,000	
Food & Beverage Sales			
Merchandise Sales			
Ticket/Entrance Fees			
Other			
Total Revenue			

I certify that all statements on this application are true and complete to the best of my knowledge.

Signature: [signature] **Title:** Executive Director

Please Print Your Name: Beverly Noerr **Date:** 4/22/26

To Be Completed by the City of Redlands

Date Received: 5/4/26 **Received By:** Jaclyn Ramirez

Notes:

City Manager Approval: City Council Approval:

Department of the Treasury
Internal Revenue Service
Tax Exempt and Government Entities
P.O. Box 2508
Cincinnati, OH 45201

Date:
03/18/2022
Employer ID number:

Person to contact:
Name: Customer Service
ID number: 31954
Telephone: (877) 829-5500
Accounting period ending:
December 31
Public charity status:
170(b)(1)(A)(vi)
Form 990 / 990-EZ / 990-N required:
Yes
Effective date of exemption:
November 15, 2020
Contribution deductibility:
Yes
Addendum applies:
No
DLN:
26053716008631

REDLANDS ART ASSOCIATION
C/O SUZANNE BURKE
215 EAST STATE STATE STREET
REDLANDS, CA 92373

Dear Applicant:

We're pleased to tell you we determined you're exempt from federal income tax under Internal Revenue Code (IRC) Section 501(c)(3). Donors can deduct contributions they make to you under IRC Section 170. You're also qualified to receive tax deductible bequests, devises, transfers or gifts under Section 2055, 2106, or 2522. This letter could help resolve questions on your exempt status. Please keep it for your records.

Organizations exempt under IRC Section 501(c)(3) are further classified as either public charities or private foundations. We determined you're a public charity under the IRC Section listed at the top of this letter.

Based on the information you submitted with your application, we approved your request for reinstatement under Revenue Procedure 2014-11. Your effective date of exemption, as listed at the top of this letter, is retroactive to your date of revocation.

If we indicated at the top of this letter that you're required to file Form 990/990-EZ/990-N, our records show you're required to file an annual information return (Form 990 or Form 990-EZ) or electronic notice (Form 990-N, the e-Postcard). If you don't file a required return or notice for three consecutive years, your exempt status will be automatically revoked.

If we indicated at the top of this letter that an addendum applies, the enclosed addendum is an integral part of this letter.

For important information about your responsibilities as a tax-exempt organization, go to www.irs.gov/charities. Enter "4221-PC" in the search bar to view Publication 4221-PC, Compliance Guide for 501(c)(3) Public Charities, which describes your recordkeeping, reporting, and disclosure requirements.

Sincerely,

Stephen A. Martin
Director, Exempt Organizations
Rulings and Agreements

Event: A Holiday Evening with Phat Cat Swinger Date: 12/4/26

PERMIT TO CLOSE STREET FOR SOCIAL EVENT(S)

Permission to close a street for an event is subject to the following requirements:

1.	**Street Closure Diagram MUST be attached. (Failure to submit diagram will result in non-issuance of permit).**
2.	**Event Flyer or Event Description MUST be attached. (Failure to submit flyer or event description will result in non-issuance of permit).**
3.	**Applicant MUST provide insurance coverage per City's requirements (see reverse)**
4.	Written permission from all residents of the effected portion of the street MUST be attached.
5.	No tables or other objects shall be placed on the street surface.
6.	No alcohol shall be consumed on the street or City right-of-way outside of a permitted area.
7.	Temporary No Parking Signs and barricades shall be supplied and posted by City Staff
8.	Affected street(s) shall remain accessible for emergency vehicles and local traffic at all times.
9.	This permit pertains only to the closing of the street(s). This permit does not relate to the type of activity, noise, or any other aspect of the event. All other applicable and appropriate ordinances and laws apply.

Permission is hereby granted to: Redlands Bowl Performing Arts
To close (street names) Eureka St and Grant St.
Between (street names) Starting by Smiley Library and Olive, Brookside to Olive
Day & date 12/4/26 **Event times -** from (time) 5 ☐ am ☑ pm to (time) 9 ☐ am ☑ pm
Address of Applicant: 168 S. Eureka St. Phone No: (909) 793-7316
Signature of Applicant: [signature] Applicant Name (print): Beverly Noerr
Condition(s);**set up & clean up time required:** Set up will begin by 4:30 pm and be picked up by 9pm.
Event Description: Holiday Christmas Concert.

FOR OFFICE USE ONLY
This permit must be signed by the Chief of Police in order to be valid.

1. [signature] Chief of Police — Date 5/19/2026
2. [signature] Municipal Utilities & Engineering Department — Date 5/21/26
3. [signature] Facilities & Community Services Department — Date 5/14/26
4. [signature] Risk Management Division — Date 5/21/26

Street Closure time: From 4 ☐ am ☒ pm To 10 ☐ am ☒ pm

Staff Notes:

RCMA Christmas Event

In anticipation of the City Council's consideration of this request, staff has compiled the following table outlining costs related to fees established by Resolution of the City Council and departmental charges pertaining to personnel and equipment resources necessary for the support of the event. The departmental charges are costs outside of normal City operations that would not be incurred by the City if the special event was not taking place.

Departmental Charges (Personnel & Equipment)	**2026-2027 Amount**	**Type**	**2025-2026 Amount**
Police Personnel[1]	$3,082.00	Hard Cost	$0.00
Fire Personnel[1]	$196.32	Hard Cost	$700.83
Facilities & Community Services Personnel[1]	$600.00	Hard Cost	$1,800.00
Personnel & Equipment Subtotal	**$3,878.32**		**$2,500.83**
Fees Established by City Council Resolution			
Park Reservation	$0.00	Soft Cost	$0.00
FCS Equipment	$1,920.00	Soft Cost	$3,360.00
Fire Equipment	$0.00	Soft Cost	$0.00
Fees Subtotal	**$1,920.00**		**$3,360.00**
Total Departmental Charges and Fees	**$5,798.32**		**$5,860.83**
	$3,878.32 **$1,920.00** **$5,798.32**	Hard Cost Soft Cost Total	**$2,500.83** **$3,360.00** **$5,860.83**

[1]*Personnel costs are calculated conservatively assuming the highest staff cost scenario. Actual costs may vary on the day of the event based on the actual staff present. Actual costs will be confirmed following the event and will be included in a reconciliation report presented to the City Council.*

The following table summarizes the total estimated costs associated with the use of City resources and waiver of fees approved for events scheduled during Fiscal Year 2026-27 to date:

TABLE 2: FY 2026-27 *Fee Waivers approved by council to date.*

Hard Costs	**Soft Costs**	**Deposits Refunded**	**Waiver Amount**	**Net Amount**
$367,972.48	$34,916.62	$0.00	$402,889.10	$402,889.10

City Council **AGENDA ITEM NO. I16.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve the use of City resources and an in-kind request in the amount of $17,922.00 related to the Redlands Turkey Trot event held on Thursday, November 26, 2026, hosted by Phoenix Hope International; approve various temporary street closures; and determine that the event is categorically exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act; and

2. I move that the City Council approve in-kind support in the amount of $17,922.00, and the temporary street closures related to the Redlands Turkey Trot event to be held on Thursday, November 26, 2026.

RECOMMENDATION:

Staff recommends that the City Council approve in-kind support in the amount of $17,922.00 for the Redlands Turkey Trot event held on Thursday, November 26, 2026, and approve the temporary street closures. Staff further recommends that the City Council determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act.

DISCUSSION:

The Facilities and Community Services Department manages the administration and issuance of permits for special events held in public areas of the City. Upon the issuance of a special event permit, the event may take place contingent on the event organizer paying the required fees. The City recognizes the value of partnering with non-profit agencies and organizations to provide beneficial services to the community. In an effort to support programs that provide community benefit, the City Council will, from time to time, consider the authorization of in-kind support, including the use of City equipment, staff and facilities for special events.

Phoenix Hope International is preparing to host the Redlands Turkey Trot (5K Race) event held on Thursday, November 26, 2026, from 7:00 a.m. to 10:00 a.m. at Sylvan Park and in the University of Redlands area. Phoenix Hope International is a non-profit organization operating out of the City of Mesa, Arizona. According to the applicant, the event is anticipated to attract approximately 5,000 attendees. This will be the 13th year Phoenix Hope International has partnered with the City of Redlands for the Turkey Trot. Phoenix Hope International has pledged to donate half of the event proceeds to the Redlands Educational Partnership (REP), which then utilizes the funds for various projects provided to schools in Redlands. The organization will also be able to further their mission and goals, which include building up schools, health clinics and other needed services in Guatemala and Nigeria.

Phoenix Hope International is requesting in-kind support valued at an estimated $17,922, including Police and Facilities and Community Services personnel, equipment, and the waiver of Sylvan Park reservation fees. The City Council previously approved $16,397.00 in in-kind support for last year's 12th annual Redlands Turkey Trot hosted by Phoenix Hope International on Thursday, November 27, 2025.

In addition, Phoenix Hope International is requesting temporary street closures for the two Turkey Trot routes (5K & 1K for children). The request for street closures for the Turkey Trot routes includes temporary closure of East Colton Avenue between Division Street and North Grove Street; Division Street between East Colton Avenue and East Park Avenue; East Park Avenue between Division Street and North University Street; North University Street between East Park Avenue and Cornell Avenue; Sylvan Boulevard between North University Street and North Grove Street; North Grove Street between Sylvan Boulevard and East Brockton Avenue; East Brockton Avenue between North Grove Street and North University Street, from the hours of 4:30 a.m. to 11:00 a.m. on Thursday, November 26, 2026.

This event qualifies for a categorical exemption from CEQA review under Section 15311(c) of the CEQA Guidelines, which applies to temporary or minor use of land having negligible or no permanent effects, including temporary placement of mobile food units, portable restrooms, or similar facilities in public parks or other facilities designed for public use.

ALTERNATIVES:

The City Council may elect to deny the request for in-kind support, deny the request for temporary street closure and direct staff accordingly.

STRATEGIC PLAN:

Priority A - Quality of Life, Beautification, Arts and Culture.

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jaclyn Ramirez, Administrative Assistant

FISCAL IMPACT

Fiscal Year: 2026/2027

Revenue Generating: Yes

Amount: $17,922.00

Budgeted Y/N: N

Account No.: N/A

Additional Appropriation Required: No

Discussion:

Please see the "Fiscal Impact" attachment for reference.

Attachments

A_Special_Event_Application_-_Turkey_Trot.pdf
B_In-Kind_Request_-_Turkey_Trot.pdf
C_2026_Traffic_Plan_-_Redlands_Turkey_Trot.pdf
D_Verification_of_Non-Profit_-_Turkey_Trot.pdf
E_Street_Closure_-_Turkey_Trot.pdf
F_Fiscal_Impact_-_Turkey_Trot.pdf

City of Redlands
35 Cajon Street, Ste. 222
Redlands, CA 92373
(909) 798-7655 ext 3

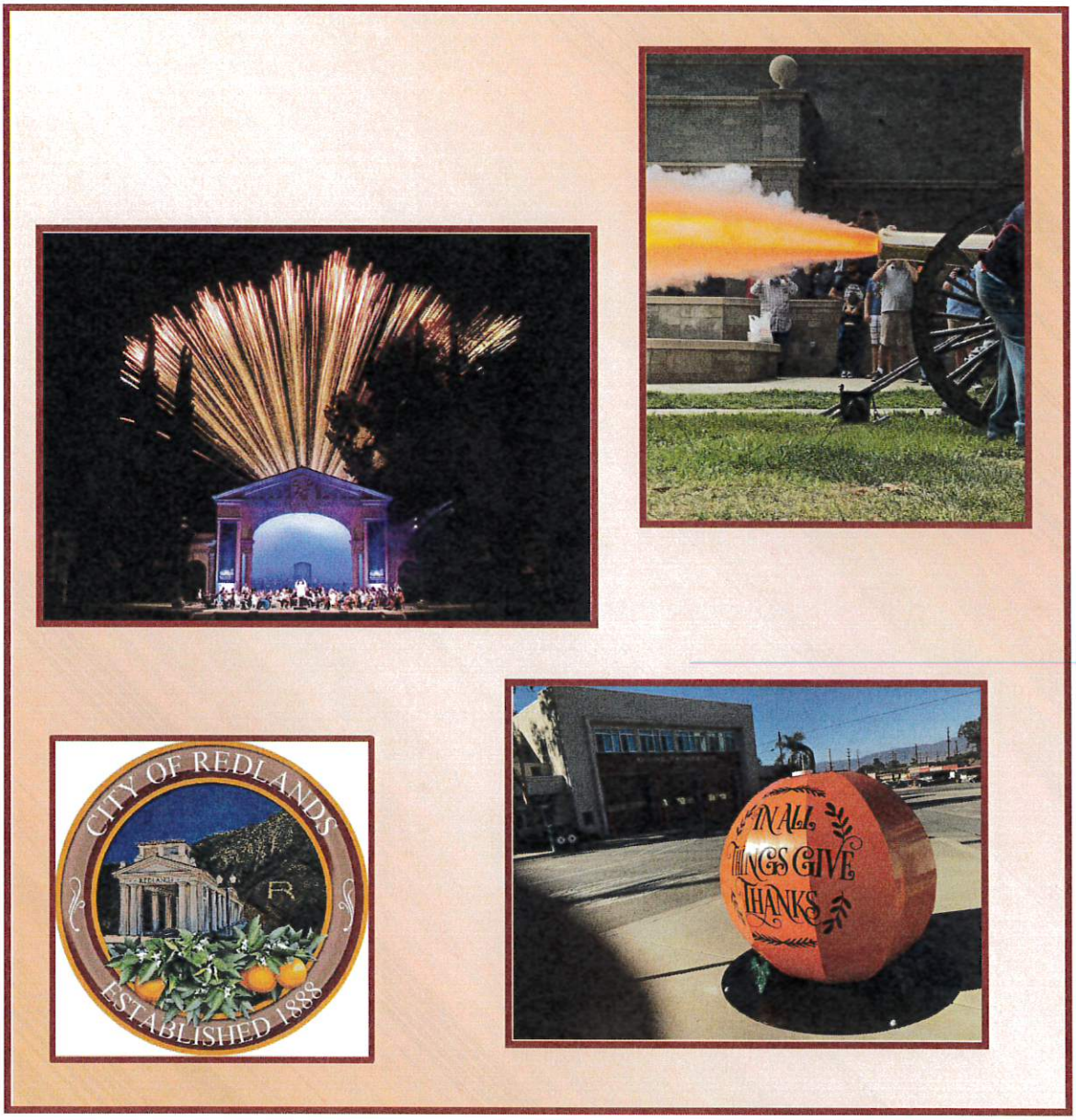
SPECIAL EVENTS PERMIT APPLICATION

EVENT: Redlands Turkey Trot

ORGANIZER: Phoenix Hope International

Date of Event: 11 / 26 / 2026

Date Submitted: 11 / 11 / 11



NOTICE TO PERMIT APPLICANT

- Completed Special Event Permit Applications **must** be submitted to the Facilities & Community Services Department a **minimum of four (4) months prior** to the date the event is scheduled to begin.
- All forms in this application package that are relevant to your event must be complete and submitted together in order to be considered.
- Applicants must conform to all requirements for maintaining liability insurance.
- Incomplete applications or applications submitted past the deadline are subject to denial of request to hold event.

SUMMARY OF EVENT

Event Title Redlands Turkey Trot

Description Running race in Redlands on Thanksgiving morning. 5K distance for most participants and a 1K race for children under 12. All proceeds goo to charitable organizations with 50% of proceeds going to Redlands schools and the Redlands Educational Partnership foundation.

Date/Time

Setup	Date 11/25/2026	Time 3 pm	Location(s) Streets near	University of Redlands
Event Starts	Date 11/26/2026	Time 7:30 am	Location(s) Streets near	U of R
Event Ends	Date 11/26/2026	Time 10 am	Location(s) Streets near	U of R
Dismantle	Date 11/26/2026	Time 10-11 am	Location(s) Streets near	U of R

*Submit a Site Plan for each venue listed

Anticipated Attendance: Total 5000 Per Day 5000

Anticipated Participants: Total 4700 Per Day 4700

CONTACTS Person(s) or Agent(s) responsible for and authorized to represent this event on all matters:

	Primary Contact:	Secondary Contact
Name:	Kent Sommer	Matt Sommer
Address:	625 Ranch Lane	14215 Bounty Way
City, State, Zip	Glendora, CA 91741	Poway, CA 92064
Phone:	714-614-7321	858-888-0218
Email:	kentsommer@gmail.com	matt.sommer@gmail.com

Name of Organization: Phoenix Hope International Is it Non-Profit? Yes
Tax I.D. #:

Yes	No	
◉	○	Is this an annual event? How many years have you been holding this event? 12 years
X	○	Street Closure(s) requested? If yes, please complete Street Closure Permit Application and Barricade Rental Form in Appendix A
○	X	Does this event involve a parade? Please complete Parade/Public Assemblies Permit Application form in Appendix A
○	X	Will you be serving alcohol? If yes, please complete <u>both</u> Alcohol Permit forms in Appendix A
○	X	Are you requesting use of the Prospect Park Sign? If yes, please complete the Sign Request form in Appendix A
○	X	Are you requesting use of the City Stage? If yes, please complete the Show Mobile Rental form in Appendix A
X	○	Vendor(s)? If yes please complete the Vendor List in Appendix A.

SITE PLAN

Your event site plan/route map should include but not be limited to:

- ❑ An outline of the entire event venue including the names of all streets or areas that are part of the venue and the surrounding area. If the event involves a moving route of any kind, indicate the direction of travel and all street or lane closures.
- ❑ The location of fencing, barriers and/or barricades. Indicate any removable fencing for emergency access.
- ❑ The provision of minimum twenty foot (20') emergency access lanes throughout the event venue.
- ❑ The location of first aid facilities and ambulances.
- ❑ The location of all stages, platforms, scaffolding, bleachers, grandstands, canopies, tents, portable toilets, booths, beer gardens, cooking areas, trash containers and dumpsters, and other temporary structures.
- ❑ A detail or close-up of the food booth and cooking area configuration including booth identification of all vendors cooking with flammable gases or barbecue grills
- ❑ Generator locations and/or source of electricity.
- ❑ Placement of vehicles and/or trailers.
- ❑ Exit locations for outdoor events that are fenced and/or locations within tents and tent structures.
- ❑ Identification of all event components that meet accessibility standards.
- ❑ A parking and/or shuttle plan for events that are likely to exceed parking lot capacity of the space you are using.
- ❑ Other related event components not listed above.

TIMELINE

Please provide a narrative and timeline of your event. You may provide this information as an attachment if necessary.

HOUR	ACTION
See traffic plan attachment	

ACCESSIBILITY PLAN

This checklist is intended to serve as a planning guideline and may not be inclusive of all City, County, State and Federal access requirements. You may attach more detailed information if necessary.

YES NO

- ☑ ☐ Will there be a Clear Path of Travel throughout your event venue? Please describe _
  See traffic plan. Entire course is on city streets and accessible to all individuals
- ☑ ☐ Have you developed a Disabled Parking and/or Transportation Plan (including the use of public transportation or shuttle services) for your event? Please describe
  Handicap parking available in all parking lots near start/finish line. No shuttle services.
- ☑ ☐ Will a minimum of 10% of portable rest rooms at your event be accessible? Please describe
  Yes
- ☑ ☐ Will all food, beverage and vending areas be accessible? Please describe
  Food beverage areas are located at the finish line and accessible to all.
- ☑ ☐ Will all signage be provided in highly contrasting colors and placed so pedestrian flow will not obstruct its visibility? Please describe
  Neon event tape used to direct runners and event participants and unobstructed by pedestrians
- ☑ ☐ If telephones are provided, will at least one telephone at each phone bank have a volume control and is hearing aid compatible? Please describe N/A
- ☑ ☐ If an information center is provided at your event will customer service representatives be available to assist disabled individuals? Please describe
  Individuals at info booth are able to assist
- ☑ ☐ If all areas of your event venue cannot be made accessible will maps or programs be made available to show the location of accessible rest rooms, parking, phones (if any), drinking fountains, and first aid stations? Please describe All areas are accessible

RESTROOM FACILITIES PLAN

You are required to provide portable rest room facilities at your event, unless you can substantiate the sufficient availability of both ADA accessible and non-accessible facilities in the immediate area of the event site which will be available to the public during your event. Indicate on your timeline when portable toilets will be set up.

Yes No

- ☑ ☑ Do you plan to provide portable rest room facilities at your event?

If yes: Total number of portable toilets 25

If no: Please explain: _____

Rest Room Company Diamond Environmental Services

Address Street 807 E Mission Road

City San Marcos State CA Zip 92069

Telephone Day 760-744-7191 Evening _____ Fax _____ Pager/Cellular _____

LIST OF VENDORS

Please provide a list of vendors, what they are there for and their business license numbers. Keep in mind that this list of vendors cannot change after the event has been approved. All must have a Redlands business license in order to participate with your event. If you need more entries, please attach a list with the same information to your event package. Vendors include all businesses either performing a service or selling at your event. All food concessioners must meet the San Bernardino Counties Department of Public Health Food Handler's and Fire Suppression requirements.

Yes	No	
☐	☒	Will items or services be sold at your event?
☒	☐	Will you have some education only (not selling a product or service) booths?
☐	☒	Will items or services sold at your event present unique liability issues (e.g. massage, etc.)?
☐	☒	Does your event include food concession and/or preparation areas?
☐	☒	Do you intend to cook food in the event area?

If yes, please specify method:

- ☐ Gas
- ☐ Electric
- ☐ Charcoal
- ☐ Other (specify) _____

VENDOR	SERVICE THEY ARE PROVIDING	REDLANDS BUSINESS LICENSE NUMBER	EDUCATIONAL INFORMATION ONLY? (Y/N)
Phoenix Hope International			Y
Redlands Educational Partnership			Y

ENTERTAINMENT PLAN

YES NO

☐ ☒ Are there any musical entertainment features related to your event?

If yes, complete the following information or provide an attachment listing all bands/performers, type of music, sound check and performance schedule.

Number of Stages _____

Number of Performers/Bands _____

Performer/Band name and music type _____

☐ ☒ Will sound checks be conducted prior to the event?

If yes, Start time _____ Finish time _____

☒ ☐ Will sound amplification be used?

If yes, Start time 7:30 am Finish time 10 am

☐ ☒ Do you plan to have a patron dance component to either live or recorded music at your event?

If yes, please describe _____

☒ ☐ Please describe the sound equipment that will be used for your event _____

_____

☐ ☒ Will inflatables, such as jumpers, or similar devices be used at your event?

If yes, please describe _____

☐ ☒ Does your event include the use of fireworks, rockets, lasers, or other pyrotechnics?

If yes, please fill out a fireworks permit also located in this packet.

If yes, please describe _____

☒ ☐ Will your event include the use of any signs, banners, decorations, or special lighting?

If yes, please describe _____

☐ ☒ Will there be massage activities at your event? If yes, please describe _____

_____

☒ ☐ Do your event plans include any, drawings or raffle opportunities?

If yes, please describe _____

ALCOHOL

Please Note: You will need to have your alcohol permit approved by Redlands city council prior to your event. A copy of your Alcohol license will be needed after city council approval, before the event.

Yes No

☐ ☒ Does your event involve the use of alcoholic beverages?

If yes, please check all that apply:

- ☐ Free/Host Alcohol
- ☐ Alcohol Sales
- ☐ Host and Sale Alcohol
- ☐ Beer
- ☐ Beer and Wine
- ☐ Beer, Wine and Distilled Spirits

Please describe your security plan to ensure the safe sale or distribution of alcohol at your event. _____

MITIGATION OF IMPACT

YES NO

☒ ☐ Have you met with the residents, businesses, places of worship, schools and other entities that may be directly impacted by your event? If yes, please attach a complete list of these entities.

If no, please explain _____

☒ ☐ Do you have a sample of the notice that you propose to distribute two weeks prior to your event? If yes, please attach.

If no, please explain _____

MARKETING AND PUBLIC RELATIONS

Yes No

☒ ☐ Will this event be marketed, promoted, or advertised in any manner?

f yes, please describe online marketing through emails to past participants, flyers to children in schools, banners on street

☐ ☒ Will there by live media coverage during the event?

f yes, please describe Unknown. None anticipated

☐ ☒ Will media vehicles be parked within the event venue?

f yes, please describe safety plan

☐ ☒ Do you have a plan to control or limit the placement and/or distribution of promotional signage, stickers, and other items?

f yes, please describe

INSURANCE REQUIREMENTS

Regardless of the event you are required to have insurance that indemnifies the city of Redlands listing the location date and time.

Name of Insurance Agency Insurance Management Group

Address Street 9610 Lima Road, Suite 102

City Fort Wayne State IN Zip 46818

Telephone Day _____ Evening _____ Fax _____ Pager/Cellular _____

Contact Name Lindsi Williams

Policy Type Commercial General Liability

Policy Amount $2,000,000/$5,000,000

Policy Number AIL0003450335202

AFFIDAVIT OF APPLICANT

I certify that the information contained in the foregoing application is true and correct to the best of my knowledge and belief that I have read, understand and agree to abide by the rules and regulations governing the proposed Special Event under the Redlands Municipal Code and I understand that this application is made subject to the rules and regulations established by the City Council and/or the City Manager or the City Manager's designee. Applicant agrees to comply will all other requirements of the City, County, State, Federal Government, and any other applicable entity which may pertain to the use of the Event venue and the conduct of the Event. In the event that a possessory interest subject to property taxation is created by virtue of this use permit, I agree to pay all possessory interest taxes and the City shall not be liable for the payment of such taxes I further agree that the payment of any such taxes shall not reduce any consideration paid to the City pursuant to this use permit. I agree to abide by these rules, and further certify that I, on behalf of the Host Organization, am also authorized to commit that organization, and therefore agree to be financially responsible for any costs and fees that may be incurred by or on behalf of the Event to the City of Redlands.

Print Name of Applicant/Host Organization Kent Sommer/Phoenix Hope International

Title Board Member

Signature Kent Sommer

Date 6/4/2026

Print Name of Professional Event Organizer _____

Title _____

Signature _____

Date _____

City of Redlands

In-Kind Support Request

Event Name: Redlands Turkey Trot

Event Date(s): 11/26/2026 **Location(s):** Area around University of Redlands

Rain Out Date: None **Beginning Time:** 7:30 am **End Time:** 10 am

Describe Your Request:

This completed form with all supporting documentation shall be submitted a minimum of 60 days prior to the scheduled event. Additional information may be attached to this application form, as needed.

Request for waiver of City fees associated with hosting this running event in Redlands, CA

Select and Describe All City Provided Services That May Apply to Your Request :

- [x] Traffic (*Personnel, equipment, cones, barricades, no-parking* — Barricades used for street closure
- [x] Police (*Public Safety Personnel*) — Officers used for event monitoring and street closures
- [ ] Fire (*Paramedics, Inspectors*)
- [ ] Parks *(Cleanup Personnel, Ball Field Lights)*
- [x] Facility — Event receptacles used for trash services

Refuse/Recycling *(Event Receptacles, Roll-Off Service)* acquired by Event Organizers through Redlands Customer Service

Section 13.65 of the Redlands Municipal Code requires that events that serve more than 2,000 individuals per day will be required to submit for review and approval a Large Venue Recycling Plan. The Quality of Life Department may require smaller events to comply with City recycling practices as a condition of waiving fees.

- [ ] Other

Group/Organization Name: Phoenix Hope International

Is your Group/Organization a Registered Non-Profit: [x] Yes [ ] No **Non-Profit Federal Tax ID Number:**

Does your Group/Organization Presently Have Liability Insurance? [x] Yes [ ] No

Please be advised that depending upon your request, you may be required to provide proof of insurance coverage in an amount determined by the City and naming the City as an additional insured.

Has your Group/Organization received fee waivers from the City in the past? Yes

Primary Contact Name & Title: Kent Sommer, Board Member

Mailing Address: 625 Ranch Lane, Glendora, CA 91741

Phone Number: 714-614-7321 **E-Mail Address:** kentsommer@gmail.com

As a part of our commitment to fiscal responsibility, the City of Redlands gathers data associated with the economic and social benefits associated with in-kind support. Please provide estimates, as applicable, for your event.

Positive outcomes for your organization from this

Our organization would be able to use more of the event proceeds to further our mission and goals, which includes building up schools, health clinics and other needed services in Guatemala and Nigeria.

Describe what economic benefit and impact this event will bring to the City:

Half of the event proceeds are donated to Redlands based organizations and charities. In the past we have donated most of those proceeds to the Redlands Educational Partnership (REP) which then utilizes the funds for the various projects they provide to the schools in Redlands. The race operating costs and City fees are paid from the event proceeds. If we did not have to pay those costs because they were waived by the City, we would be able to donate more of our proceeds to the aforementioned charities.

In April 2002, the City Council adopted Resolution No. 6038, which encourages groups or organizations requesting in-kind support from the City to use local businesses when procuring goods and services associated with the event. Receipts will need to be submitted through a follow up form. Failure to submit post event documentation (within 15 days) may affect future requests.

	Proposed Event	Previous Event Actuals	Vendors
Attendance: Redlands Residents	3500	3200	1
Attendance: Non-Residents	1500	1500	1
Food & Beverage Sales	$1000	$1000	$1000
Merchandise Sales	$250	$250	None
Ticket/Entrance Fees	$30/adult; $15/child	$30/adult; $15/child	None
Other	None	None	None
Total Revenue	$100,000	$100,000	$1000

I certify that all statements on this application are true and complete to the best of my knowledge.

Signature: Kent Sommer **Title:** Board Member

Please Print Your Name: Kent Sommer **Date:** 6/4/2026

To Be Completed by the City of Redlands

Date Received: 6/4/26 **Received By:** Jaclyn. Ramirez

Notes:

City Manager Approval: City Council Approval:

REDLANDS TURKEY TROT

Thursday, November 26, 2026

8 a.m.

Traffic Plan

Phoenix Hope International

Event Information

Event Organizer: Phoenix Hope International

Race Contact: Kent Sommer
(714) 614-7321
kentsommer@gmail.com

Race proceeds benefitting the following organizations:

Phoenix Hope International

Redlands Educational Partnership

Inland Harvest Food Bank

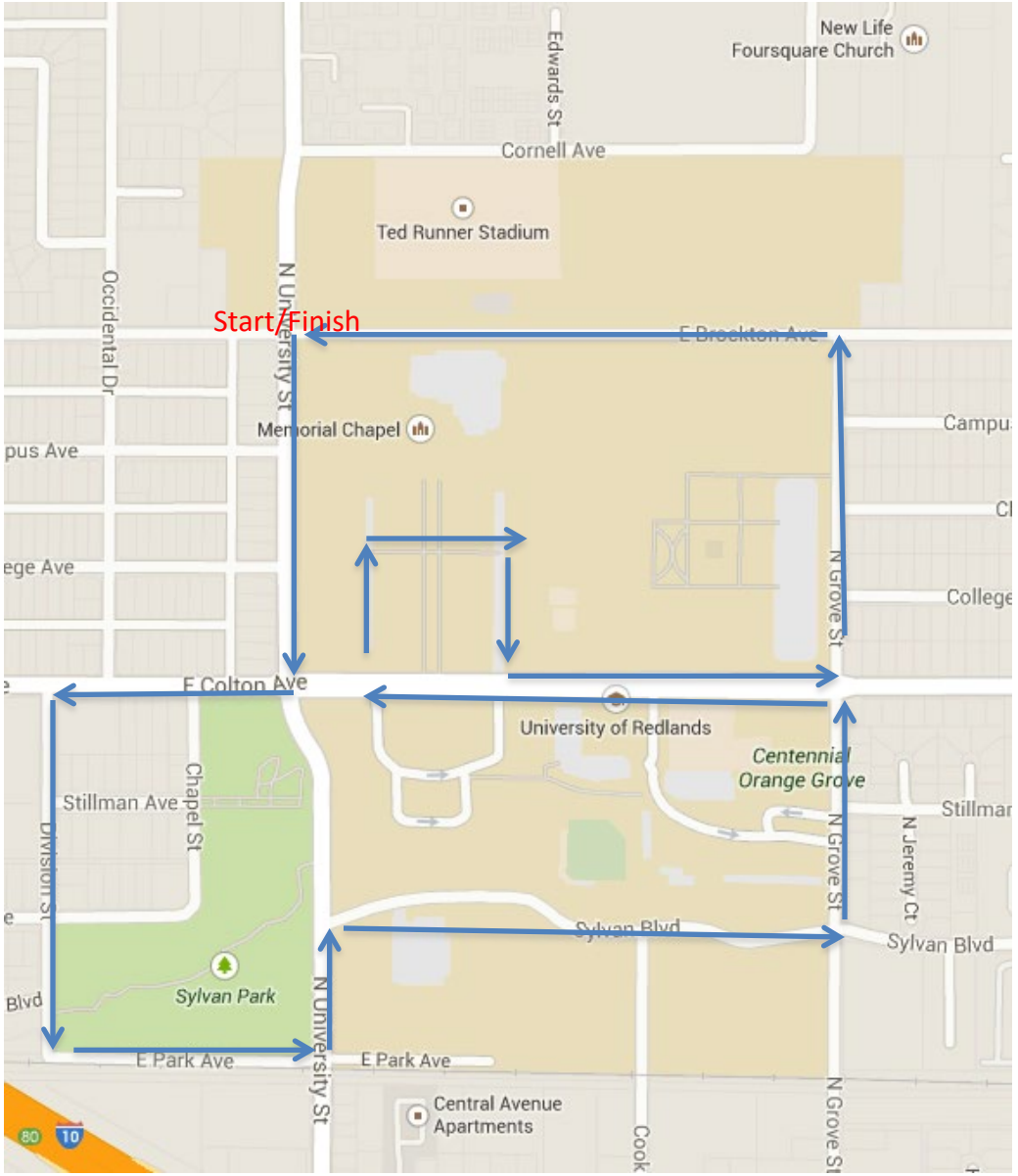
Race Day Schedule

Morning Check-In:	7 a.m.
Kids 1K Start:	7:45 a.m.
5K Race Start:	8 a.m.
Last Finisher:	9:30 a.m.
Awards:	9:30 a.m.
Clean-up:	10-11 a.m.

5K Course

The 5k and 1k course is different than prior years:

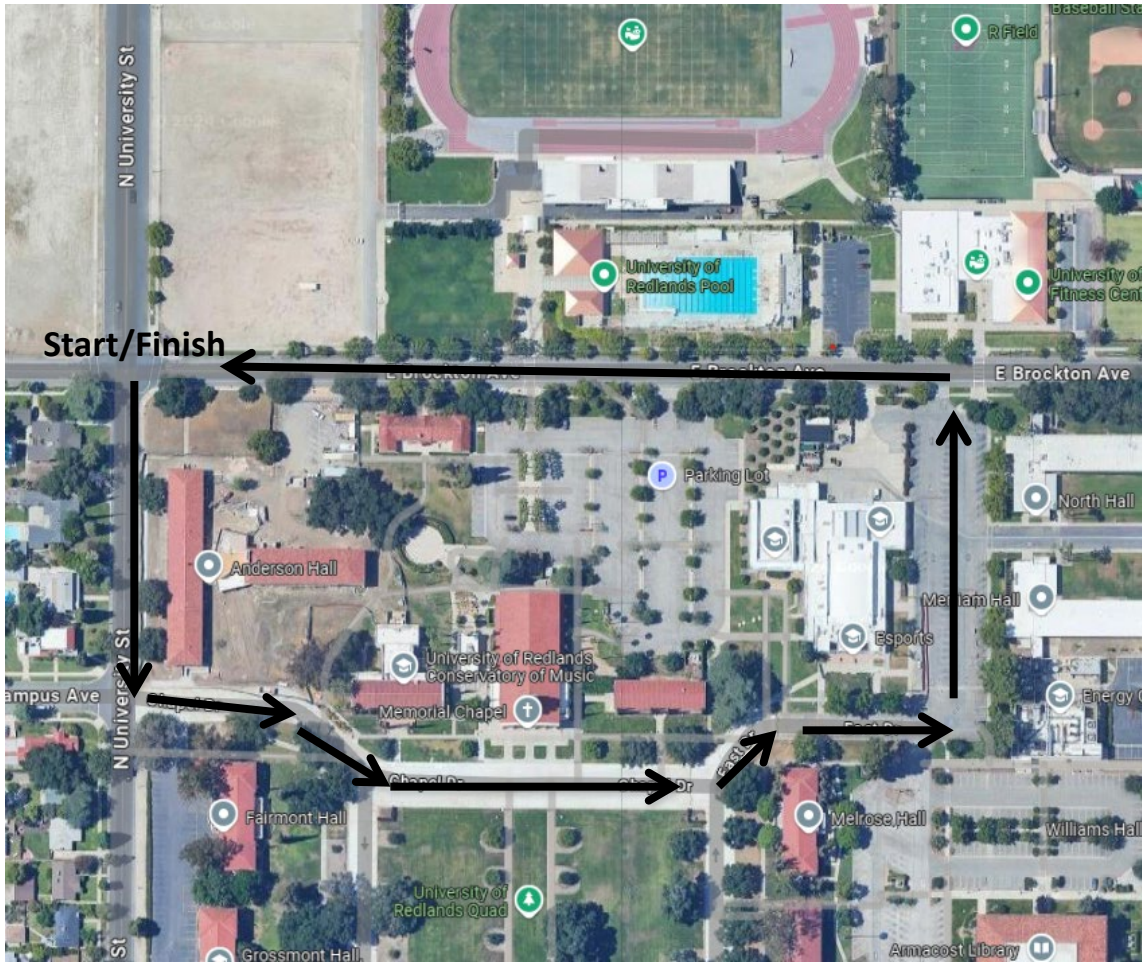
1. Start at corner of University St and Brockton Ave
2. Participants will run south on University St.
3. West on Colton Ave.
4. South on Division St.
5. East on Park Ave
6. North on University St.
7. East on Sylvan Blvd
8. North on Grove St.
9. East on Colton Ave
10. North on West Drive
11. East on Chapel Dr.
12. South on East Drive
13. East on Colton Ave
14. North on Grove St
15. West on Brockton Ave. to the Finish



Kids' 1K Course

The kids (12 and under) 1K fun run course will be as follows:

1. Start the corner of University St and E Brockton Ave
2. Participants will run south on University St.
3. East on Chapel Drive
4. Continue east on East Dr.
5. Through the parking lot to E Brockton Ave.
6. West on Brockton Ave to the Finish



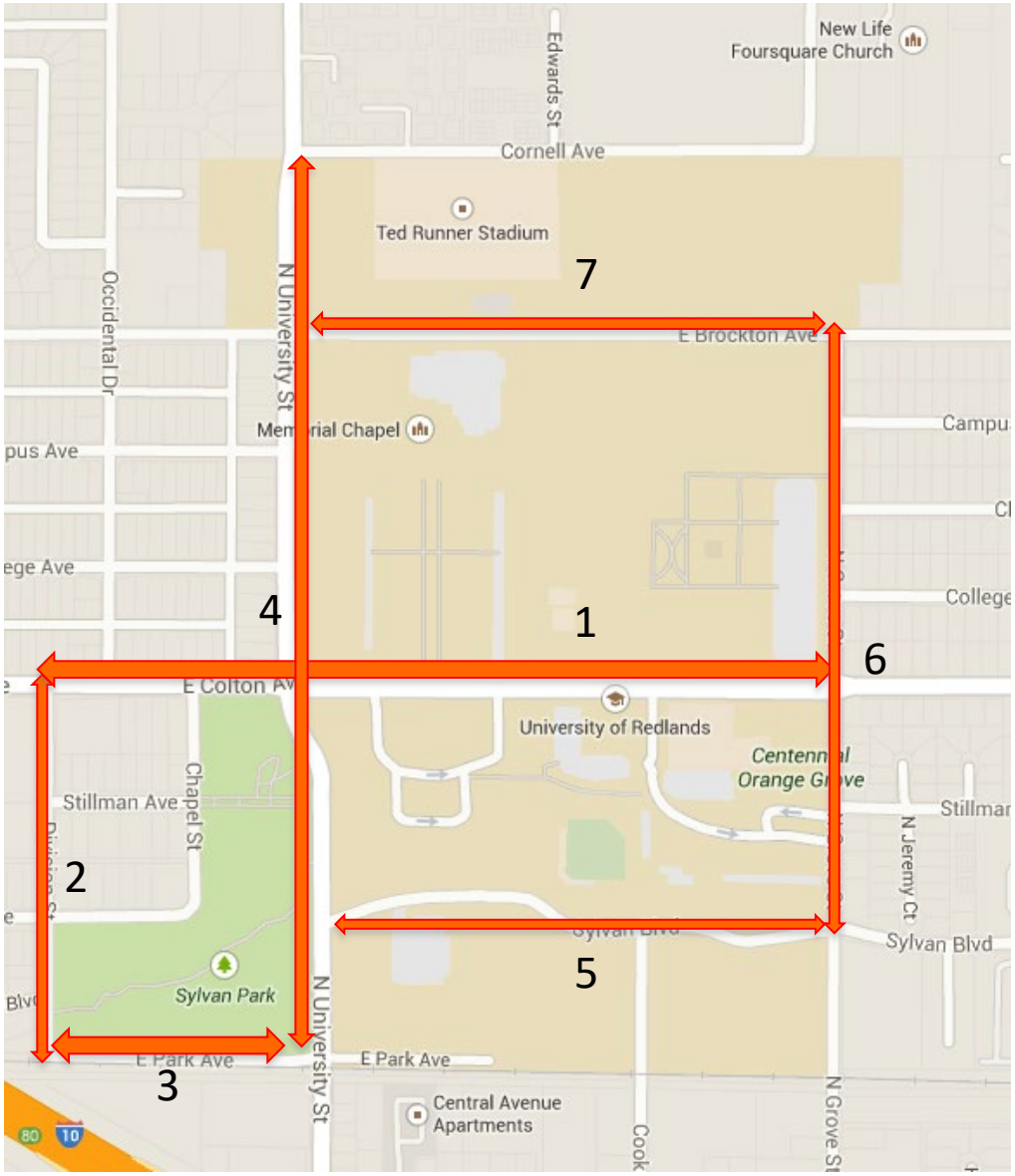
Street Closures

The following street closures are proposed for the event.

1. Colton Ave between Division Street and Grove St.
2. Division St. between E Colton St. and Park Ave.
3. E Park Ave. between Division Street and University Street.
4. N University Street between E Park Ave and Cornell Ave.
5. Sylvan Blvd between N University St and N Grove St.
6. N Grove St between Sylvan Blvd and E Brockton Ave
7. E Brockton Ave between N Grove St and N University St.

Street closures will likely last two hours from 7:30 (15 minutes before the 1K race begins) to 9:30 a.m. (estimated time when last runner will finish the 5K).

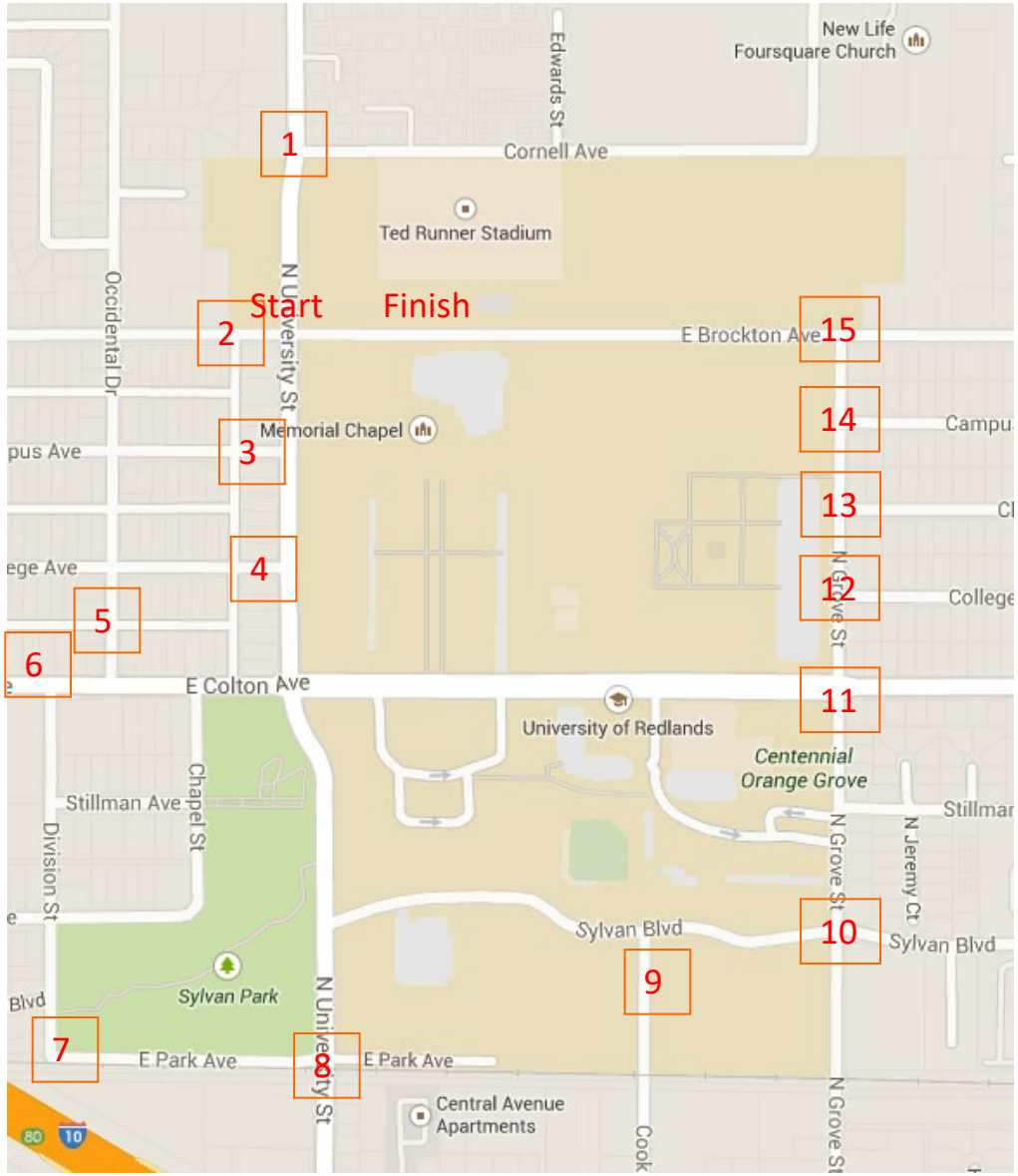
Roads will remain open and accessible to emergency vehicles as well as any residents that live on a street that is closed.



Traffic Monitor Locations

Traffic Monitor Intersections:

1. Cornell Ave and University St
2. University St and Brockton Ave
3. University St and Campus Ave
4. University St. and College Ave
5. Colton Ave and Occidental Dr
6. Colton Ave and Division St
7. Division St and Park Ave
8. University St and Park Ave
9. Sylvan Ave Blvd and Cook St
10. Grove St. and E. Sylvan Blvd
11. Grove St and Colton Ave
12. Grove St and College Ave
13. Grove St and Clock St
14. Grove St and Campus Ave
15. Grove St and Brockton Ave



Traffic Monitors Continued

All monitors will be provided by Phoenix Hope International/Race Organizer.

All monitors will be over 18 years old, will wear safety reflector vests, and will all be trained in traffic safety for the event.

Monitors will have radios and direct communication with the race info/headquarters located in Sylvan park. Any incidents will be immediately reported to race info so that appropriate personnel are notified and can be dispatched to area if needed.

Monitors will be familiar with the course as well as surrounding area in order to instruct motorists of available detours around the event.

Start/Finish Line

The race start is on University St. near the Brockton Ave.

The finish line will be on Brockton Ave near University St.

An inflatable arch is placed at the start and finish line

There are various 10x10 canopies (“EZ Ups”) placed in the near the start/finish line area. One EZ up is near the finish line and used by the timing company. Other EZ ups to be placed in TRS parking lot or Serrano Lawn for race day check-in, t-shirt distribution and volunteer check in. Small staging area also set up for handing out post-race awards.

Port-a-potties are purchased for the event and are placed near the start/finish area in TRS parking lot.

Safety

First Aid

- One EMT located at start/finish line.
- Nurse or other medical personnel on-site at first aid booth to treat light injuries (muscle, strains, sprains, cramps, etc.)
- Area Urgent Care / ER notified of event
- Any other provisions/recommendations from the City

Post race Overview

- Potential post race expo involving local vendors/sponsors
- Hand out participant t-shirts
- Awards (Thanksgiving pies) to all male/female overall winners and age group winners
- Appropriate health permits (as needed) for post-race food (bananas and orange slices)
- Port-a-potties + hand wash stations at start/finish line
- Clean-up area and dispose of trash
- Return all barricades to City Yard
- Last few years the roads were reopened by 9:30 a.m. and entire event was cleaned up and all participants and race organizers were gone by 11 a.m.

INTERNAL REVENUE SERVICE
P. O. BOX 2508
CINCINNATI, OH 45201

DEPARTMENT OF THE TREASURY

Date: SEP 18 2013

Employer Identification Number:

DLN:
17053200307032
Contact Person:
DIANE M GENTRY ID# 31361
Contact Telephone Number:
(877) 829-5500
Accounting Period Ending:
December 31
Public Charity Status:
170(b)(1)(A)(vi)
Form 990 Required:
Yes
Effective Date of Exemption:
June 10, 2010
Contribution Deductibility:
Yes
Addendum Applies:
No

PHOENIX HOPE INTERNATIONAL
C/O PARKER FILLMORE
1460 N GAYLORD CIR
MESA, AZ 85213

Dear Applicant:

We are pleased to inform you that upon review of your application for tax exempt status we have determined that you are exempt from Federal income tax under section 501(c)(3) of the Internal Revenue Code. Contributions to you are deductible under section 170 of the Code. You are also qualified to receive tax deductible bequests, devises, transfers or gifts under section 2055, 2106 or 2522 of the Code. Because this letter could help resolve any questions regarding your exempt status, you should keep it in your permanent records.

Organizations exempt under section 501(c)(3) of the Code are further classified as either public charities or private foundations. We determined that you are a public charity under the Code section(s) listed in the heading of this letter.

Please see enclosed Publication 4221-PC, Compliance Guide for 501(c)(3) Public Charities, for some helpful information about your responsibilities as an exempt organization.

Sincerely,

Director, Exempt Organizations

Enclosure: Publication 4221-PC

Letter 947 (DO/CG)

Event: Redlands Turkey Trot

PERMIT TO CLOSE STREET FOR SOCIAL EVENT(S)

Permission to close a street for an event is subject to the following requirements:

1.	**Street Closure Diagram MUST be attached. (Failure to submit diagram will result in non-issuance of permit).**
2.	**Event Flyer or Event Description MUST be attached. (Failure to submit flyer or event description will result in non-issuance of permit).**
3.	**Applicant MUST provide insurance coverage per City's requirements (see reverse)**
4.	Written permission from all residents of the effected portion of the street MUST be attached.
5.	No tables or other objects shall be placed on the street surface.
6.	No alcohol shall be consumed on the street or City right-of-way outside of a permitted area.
7.	Temporary No Parking Signs and barricades shall be supplied and posted by City Staff
8.	Affected street(s) shall remain accessible for emergency vehicles and local traffic at all times.
9.	This permit pertains only to the closing of the street(s). This permit does not relate to the type of activity, noise, or any other aspect of the event. All other applicable and appropriate ordinances and laws apply.

Permission is hereby granted to: Kent Sommer/Phoenix Hope International

To close (street names) See traffic plan

Between (street names) _____

On (date) 11/26/26 **Event times -** from (time) 7 ☑ am ☐ pm to (time) 10 ☑ am ☐ pm

Address of Applicant: 625 Ranch Lane, Glendora, CA 91741

Signature of Applicant: Kent Sommer Phone No. 714-614-7321

Condition(s): Set up at 5 am; clean up 10-11 am

Event Description: 5k run in Redlands on Thanksgiving morning

FOR OFFICE USE ONLY

This permit must be signed by the Chief of Police in order to be valid.

1. _____ Chief of Police — Date 6/11/26
2. _____ Municipal Utilities & Engineering Department — Date _____
3. _____ Facilities & Community Services Department — Date 6/9/26
4. _____ Risk Management Division — Date 6/24/26

Street Closure time: From 4:30 ☒ am ☐ pm To 11 ☒ am ☐ pm

Staff Notes:

In anticipation of the City Council's consideration of this request, staff has compiled the following table outlining costs related to fees established by Resolution of the City Council and departmental charges pertaining to personnel and equipment resources necessary for the support of the event. The departmental charges are costs outside of normal City operations that would not be incurred by the City if the special event was not taking place.

Departmental Charges (Personnel & Equipment)	**2026-2027 Amount**	**Type**	**2025-2026 Amount**
Police Personnel[1]	$14,056.00	Hard Cost	$13,551.00
Fire Personnel[1]	$0.00	Hard Cost	$0.00
Facilities & Community Services Personnel[1]	$1,800.00	Hard Cost	$2,700.00
Personnel & Equipment Subtotal	**$15,856.00**		**$16,251.00**
Fees Established by City Council Resolution			
Park Reservation	$146.00	Soft Cost	$146.00
FCS Equipment	$1,920.00	Soft Cost	$0.00
Fire Equipment	$0.00	Soft Cost	$0.00
Fees Subtotal	**$2,066.00**		**$146.00**
Total Departmental Charges and Fees	**$17,922.00**		**$16,397.00**
	$15,856.00 **$2,066.00** **$17,922.00**	Hard Cost Soft Cost Total	**$16,251.00** **$146.00** **$16,397.00**

[1]*Personnel costs are calculated conservatively assuming the highest staff cost scenario. Actual costs may vary on the day of the event based on the actual staff present. Actual costs will be confirmed following the event and will be included in a reconciliation report presented to the City Council.*

The following table summarizes the total estimated costs associated with the use of City resources and waiver of fees approved for events scheduled during Fiscal Year 2026-27 to date:

TABLE 2: FY 2026-27 Fee Waivers to date

Hard Costs	**Soft Costs**	**Deposits Refunded**	**Waiver Amount**	**Net Amount**
$367,972.48	$34,916.62	$0.00	$402,889.10	$402,889.10

City Council **AGENDA ITEM NO. I17.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Authorize the sale and consumption of alcoholic beverages and temporary street closures related to the REVEL Big Bear Marathon event held on Saturday, November 7, 2026, by the Brooksee Foundation and determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that the approval of the event activities is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act; and

2. I move that the City Council authorize the sale and consumption of alcoholic beverages and the temporary closure of streets for the Brooksee Foundation’s REVEL Big Bear Marathon event to be held on Saturday, November 7, 2026.

RECOMMENDATION:

Staff recommends that the City Council authorize the sale and consumption of alcoholic beverages and related street closures for the REVEL Big Bear Marathon event to be held on Saturday, November 7, 2026. Staff further recommends that the City Council determine that the approval of the event is exempt from environmental review pursuant to Section 15311(c) of the State's Guidelines implementing the California Environmental Quality Act.

DISCUSSION:

The Facilities and Community Services Department manages the administration and issuance of permits for special events held in public areas of the City. The Brooksee Foundation, a nonprofit organization based in Highland, Utah, is preparing to host the ninth annual REVEL Big Bear Marathon on Saturday, November 7, 2026 with the event starting at 6:00 am and continuing through 1:00 pm. The Brooksee Foundation is requesting a temporary street closure along East San Bernardino Avenue between Wabash Avenue and Dearborn Street. The marathon and half-marathon begin in Angelus Oaks and ends in Redlands along San Bernardino Avenue adjacent to the Redlands Sports Park. Setup for the event, including the street closure, will be on Friday, November 6, 2026, starting at 7:00 am, with the street closure in effect until 5:00 pm on Saturday, November 7th, 2026. According to the Brooksee Foundation, the anticipated attendance for the annual REVEL Big Bear Marathon event is approximately 3,000 attendees.

The Brooksee Foundation is also requesting permission to sell and allow the consumption of alcoholic beverages at the event. The Brooksee Foundation serves one beer to each race participant as a courtesy and gives the option to purchase additional beer for the race participants only. Proceeds from each REVEL runner's entry fee are donated to local nonprofit organizations geared towards health and environmental causes. The City Council approved a similar request on November 8, 2025. City Council approval is necessary to authorize the sale and consumption of alcohol for this event due to its location. Staff's approval authority is limited to enclosed public areas in public parks as defined by Resolution No. 7559.

This event qualifies for a categorical exemption from CEQA review under Section 15311(c) of the CEQA Guidelines, which applies to temporary or minor use of land having negligible or no permanent effects, including temporary placement of mobile food units, portable restrooms, or similar facilities in public parks or other facilities designed for public use.

ALTERNATIVES:

The City Council may elect not to approve the request for the sale and consumption of alcoholic beverages, and the temporary closure of streets and provide alternative direction to staff.

STRATEGIC PLAN:

Priority A - Quality of Life, Beautification, Arts and Culture.

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jaclyn Ramirez, Administrative Assistant

FISCAL IMPACT

Fiscal Year: FY 2026/27

Revenue Generating: No

Amount: N/A

Budgeted Y/N: N

Account No.: N/A

Additional Appropriation Required: No

Discussion:

There is no fiscal impact related to this event, as all fees will be paid by the non-profit.

Attachments

A_Special_Event_Application_-_REVEL_Big_Bear_Marathon.pdf
B_Street_Closure_Permit_-_REVEL_Big_Bear_Marathon.pdf
C_Event_Map_-_REVEL_Big_Bear.pdf
D_DLA_Application_-_Big_Bear_Marathon.pdf
E_Verification_of_non-profit_-_REVEL_Big_Bear_Marathon.pdf
F_2026_Big_Bear_Operations_Plan_-_REVEL_Bif_Bear_Marathon.pdf
G_Resolution_No_7559.pdf

City of Redlands
35 Cajon Street, Ste. 222
Redlands, CA 92373
(909) 798-7655 ext 3

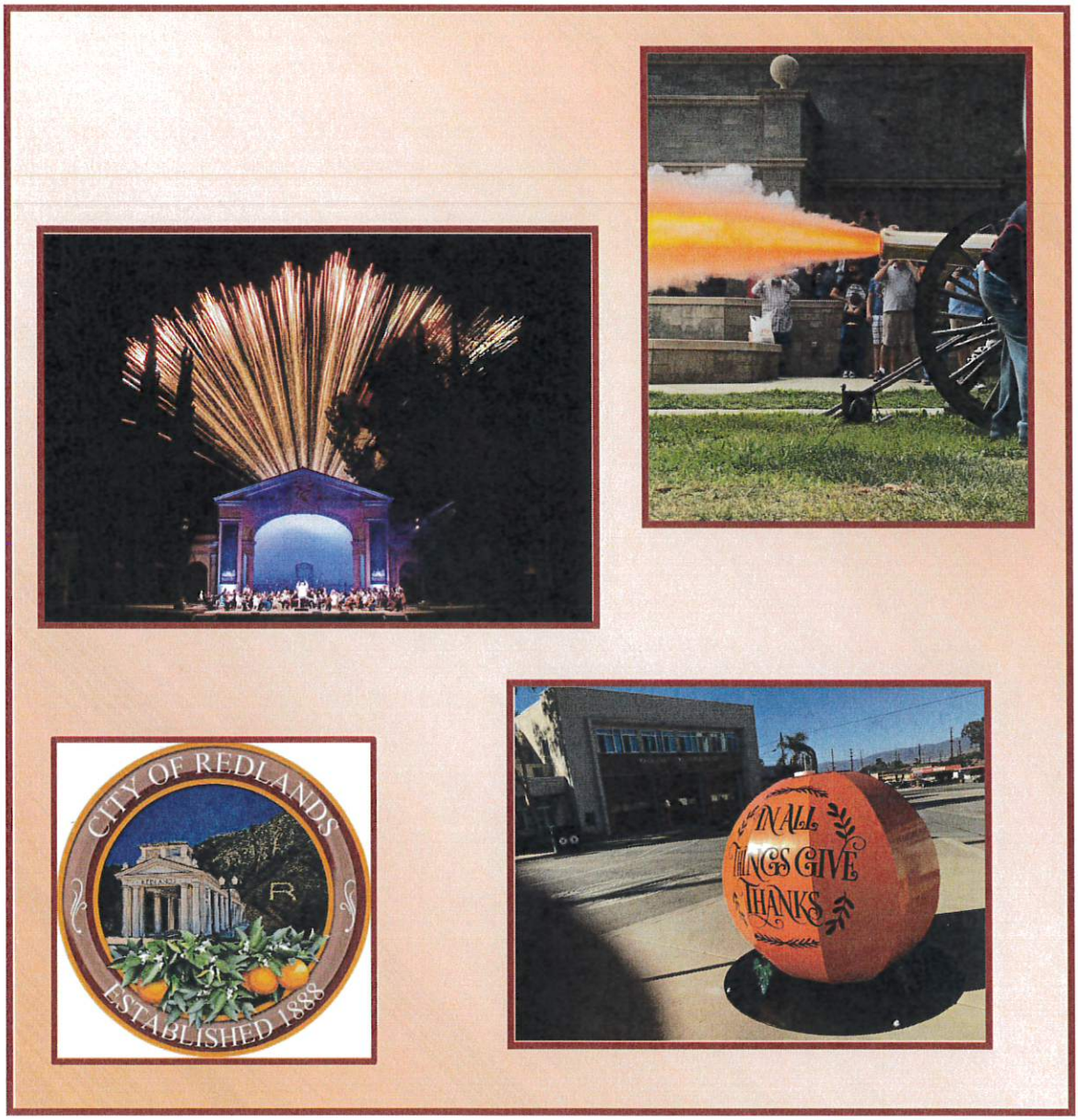
SPECIAL EVENTS PERMIT APPLICATION

EVENT: REVEL Big Bear Marathon & Half

ORGANIZER: Brooksee, Inc

Date of Event: 11 /7 /2026

Date Submitted: 08 / 04 / 2024



NOTICE TO PERMIT APPLICANT

- Completed Special Event Permit Applications **must** be submitted to the Facilities & Community Services Department a **minimum of four (4) months prior** to the date the event is scheduled to begin.
- All forms in this application package that are relevant to your event must be complete and submitted together in order to be considered.
- Applicants must conform to all requirements for maintaining liability insurance.
- Incomplete applications or applications submitted past the deadline are subject to denial of request to hold event.

SUMMARY OF EVENT

Event Title REVEL Big Bear Marathon & Half

Description The marathon will start at CODES School Outdoor Science (Mile High Pines) and run down Highway 38 and into the City of Redlands and end at Redlands Sports Complex. The Half Marathon will start on the Valley of the Falls Dr. approximately 1/2 mile up from the intersection of Highway 38 and Valley of the Falls Dr. and join the marathon on Highway 38.

Date/Time

E. San Bernardino Ave (Between Wabash Ave and Dearborn St.) for all dates and times noted.

Setup	Date 11/6/26	Time 7:00-10:00 PM	Location(s)	
Event Starts	Date 11/7/26	Time 6:00 am	Location(s)	
Event Ends	Date 11/7/26	Time 1:00 pm	Location(s)	
Dismantle	Date 11/7/26	Time 1:00-5:00pm	Location(s)	

*Submit a Site Plan for each venue listed

Anticipated Attendance: Total _____ Per Day _____

Anticipated Participants: Total 3000 Per Day 11/7

CONTACTS Person(s) or Agent(s) responsible for and authorized to represent this event on all matters:

	Primary Contact:	Secondary Contact
Name:	Anna Skoien	Rob Bigelow
Address:	374 S 671 W	374 S 671 W
City, State, Zip	Pleasant Grove, UT 84062	Pleasant Grove, UT 84062
Phone:	720-467-2188	801-362-5501
Email:	anna@brooksee	rob@brooksee

Name of Organization: Brooksee Foundation Is it Non-Profit? Yes

Tax I.D. #:

Yes	No	
●	○	Is this an annual event? How many years have you been holding this event? 8
●	○	Street Closure(s) requested? If yes, please complete Street Closure Permit Application and Barricade Rental Form in Appendix A
○	●	Does this event involve a parade? Please complete Parade/Public Assemblies Permit Application form in Appendix A
●	○	Will you be serving alcohol? If yes, please complete both Alcohol Permit forms in Appendix A
○	●	Are you requesting use of the Prospect Park Sign? If yes, please complete the Sign Request form in Appendix A
○	●	Are you requesting use of the City Stage? If yes, please complete the Show Mobile Rental form in Appendix A
●	○	Vendor(s)? If yes please complete the Vendor List in Appendix A.

SITE PLAN

Your event site plan/route map should include but not be limited to:

- ❑ An outline of the entire event venue including the names of all streets or areas that are part of the venue and the surrounding area. If the event involves a moving route of any kind, indicate the direction of travel and all street or lane closures.
- ❑ The location of fencing, barriers and/or barricades. Indicate any removable fencing for emergency access.
- ❑ The provision of minimum twenty foot (20') emergency access lanes throughout the event venue.
- ❑ The location of first aid facilities and ambulances.
- ❑ The location of all stages, platforms, scaffolding, bleachers, grandstands, canopies, tents, portable toilets, booths, beer gardens, cooking areas, trash containers and dumpsters, and other temporary structures.
- ❑ A detail or close-up of the food booth and cooking area configuration including booth identification of all vendors cooking with flammable gases or barbecue grills
- ❑ Generator locations and/or source of electricity.
- ❑ Placement of vehicles and/or trailers.
- ❑ Exit locations for outdoor events that are fenced and/or locations within tents and tent structures.
- ❑ Identification of all event components that meet accessibility standards.
- ❑ A parking and/or shuttle plan for events that are likely to exceed parking lot capacity of the space you are using.
- ❑ Other related event components not listed above.

TIMELINE

Please provide a narrative and timeline of your event. You may provide this information as an attachment if necessary.

HOUR	ACTION
see attached document	

SECURITY PLAN

YES NO

❑ ❑ Have you hired a licensed professional security company to develop and manage your event's security plan? If yes, you are required to provide a copy of the security company's valid Private Patrol Operator's License issued by the State of California.

Security Organization ASP Security Services

Address Street 1255 W Colton Ave #537

City Redlands State CA Zip 92734

Telephone Day 888-632-7099 Evening _____ Fax _____ Pager/Cellular _____

Private Patrol Operator License# 18031

Please describe your security plan including crowd control, internal security or venue safety, or attach the plan to this application. See attached plan

MEDICAL PLAN

Any event that has physical activity or is a race and has above 50 people requires amedical plan.

YES NO

❑ ❑ Have you hired a licensed professional emergency medical services provider to develop and manage your event's medical plan?

If yes, please list:

Medical Services Provider Prevent Medical Solutions

Address Street 2260 S Vista Ave

City Bloomington State CA Zip 92316

Telephone Day 909-533-9306 Evening _____ Fax _____ Pager/Cellular _____

Please describe your medical plan including your communications plan, the number, certification levels (MD, RN, Paramedic, EMT) and types of resources that will be at your event and the manner in which they will be managed and deployed. Your plan should include hours of setup and dismantle of medical aid areas. You may attach the plan to this application if necessary.

See attached plan

ACCESSIBILITY PLAN

This checklist is intended to serve as a planning guideline and may not be inclusive of all City, County, State and Federal access requirements. You may attach more detailed information if necessary.

YES NO

☒ ☐ Will there be a Clear Path of Travel throughout your event venue? Please describe _
Our venue is designed and spaced out to allow runners easy access through runner services and out into vendor's space, with room to mingle. .See attached finish line map for more details.

☒ ☐ Have you developed a Disabled Parking and/or Transportation Plan (including the use of public transportation or shuttle services) for your event? Please describe
Shuttle services will bring runners from the finish venue at Redlands Sports Complex back to their cars at 650 E Hospitality Lane. See the shuttle map for more details.

☒ ☐ Will a minimum of 10% of portable rest rooms at your event be accessible? Please describe
Port-a-pots are placed in the north west section of the venue, easily accessible to participants and spectators.

☒ ☐ Will all food, beverage and vending areas be accessible? Please describe
All food and beverages will be located inside the venue and are easily accessible, see map for details.

☒ ☐ Will all signage be provided in highly contrasting colors and placed so pedestrian flow will not obstruct its visibility? Please describe
We have raised feather flags with designated signage that over 12' tall, colored in orange, blue and red. They do not obstruct view or flow.

☐ ☒ If telephones are provided, will at least one telephone at each phone bank have a volume control and is hearing aid compatible? Please describe
N/A

☐ ☒ If an information center is provided at your event will customer service representatives be available to assist disabled individuals? Please describe
There is no information center but staff are in brightly colored vests to assist. There is also accessible parking for access to the venue.

☒ ☐ If all areas of your event venue cannot be made accessible will maps or programs be made available to show the location of accessible rest rooms, parking, phones (if any), drinking fountains, and first aid stations? Please describe Venue is accessible, map is provided in advance and signage is

RESTROOM FACILITIES PLAN

You are required to provide portable rest room facilities at your event, unless you can substantiate the sufficient availability of both ADA accessible and non-accessible facilities in the immediate area of the event site which will be available to the public during your event. Indicate on your timeline when portable toilets will be set up.

Yes No

☒ ☐ Do you plan to provide portable rest room facilities at your event?

If yes: Total number of portable toilets 20 (2 ADAs)

If no: Please explain:

Rest Room Company United Site Services

Address Street 2323 West Baseline Raod

City San Bernardino State CA Zip 92410

Telephone Day 866-449-8607 Evening Fax Pager/Cellular

LIST OF VENDORS

Please provide a list of vendors, what they are there for and their business license numbers. Keep in mind that this list of vendors cannot change after the event has been approved. All must have a Redlands business license in order to participate with your event. If you need more entries, please attach a list with the same information to your event package. Vendors include all businesses either performing a service or selling at your event. All food concessioners must meet the San Bernardino Counties Department of Public Health Food Handler's and Fire Suppression requirements.

Yes	No	
☒	☐	Will items or services be sold at your event?
☒	☐	Will you have some education only (not selling a product or service) booths?
☐	☒	Will items or services sold at your event present unique liability issues (e.g. massage, etc.)?
☐	☒	Does your event include food concession and/or preparation areas?
☐	☒	Do you intend to cook food in the event area?

If yes, please specify method:

- ☐ Gas
- ☐ Electric
- ☐ Charcoal
- ☐ Other (specify) _____

VENDOR	SERVICE THEY ARE PROVIDING	REDLANDS BUSINESS LICENSE NUMBER	EDUCATIONAL INFORMATION ONLY? (Y/N)
List to be provided			

ENTERTAINMENT PLAN

YES NO

☐ ■ Are there any musical entertainment features related to your event?

If yes, complete the following information or provide an attachment listing all bands/performers, type of music, sound check and performance schedule.

Number of Stages _____

Number of Performers/Bands _____

Performer/Band name and music type _____

☒ ☐ Will sound checks be conducted prior to the event?

If yes, Start time 6:00am Finish time 6:30am

☒ ☐ Will sound amplification be used?

If yes, Start time 6:30am Finish time 1:00pm

☐ ☒ Do you plan to have a patron dance component to either live or recorded music at your event?

If yes, please describe _____

☒ ☐ Please describe the sound equipment that will be used for your event Sound mixer and 4-6 speaker to play music and make announcements as runners cross the finish line.

☐ ☒ Will inflatables, such as jumpers, or similar devices be used at your event?

If yes, please describe

☐ ☒ Does your event include the use of fireworks, rockets, lasers, or other pyrotechnics?

If yes, please fill out a fireworks permit also located in this packet.

If yes, please describe

☒ ☐ Will your event include the use of any signs, banners, decorations, or special lighting?

If yes, please describe Yes, banners and signs will be displayed as decoration and informational purposes.

☒ ☐ Will there be massage activities at your event? If yes, please describe

There may be complimentary massage (10-15) for runners post-race

☐ ☒ Do your event plans include any, drawings or raffle opportunities?

If yes, please describe _____

ALCOHOL

Please Note: You will need to have your alcohol permit approved by Redlands city council prior to your event. A copy of your Alcohol license will be needed after city council approval, before the event.

Yes No

☑ ☐ Does your event involve the use of alcoholic beverages?

If yes, please check all that apply:

- ☐ Free/Host Alcohol
- ■ Alcohol Sales
- ☐ Host and Sale Alcohol
- ■ Beer
- ☐ Beer and Wine
- ☐ Beer, Wine and Distilled Spirits

Please describe your security plan to ensure the safe sale or distribution of alcohol at your event. _____

Runners have the chance to purchase a beer before the event, proof of this purchase is given or sticker on their bib. Once they are at the finsih line they can go over to the beer garden, wh security gaurds (security is staged at the ingress/egress of the beer gardent). With confirmatio allowed to enter the beer garden.

MITIGATION OF IMPACT

YES NO

☒ ☐ Have you met with the residents, businesses, places of worship, schools and other entities that may be directly impacted by your event? If yes, please attach a complete list of these entities.

If no, please explain _____

☒ ☐ Do you have a sample of the notice that you propose to distribute two weeks prior to your event? If yes, please attach.

If no, please explain _____

MARKETING AND PUBLIC RELATIONS

Yes No

☒ ☐ Will this event be marketed, promoted, or advertised in anymanner?

f yes, please describe Social media (facebook and instagram) and internal marketing ema

☒ ☐ Will there by live media coverage during the event?

f yes, please describe A press release is sent prior to the event and local media may resp

☐ ☒ Will media vehicles be parked within the event venue?

f yes, please describe safety plan No, they cannot park in the venue.

☒ ☐ Do you have a plan to control or limit the placement and/or distribution of promotional signage, stickers, and other items?

f yes, please describe Distribution of these items is limited to paid-vendors and are only h respective booths.

INSURANCE REQUIREMENTS

Regardless of the event you are required to have insurance that indemnifies the city of Redlands listing the location date and time.

Name of Insurance Agency HCC Speciality

Address Street 401 Edgewater Place, Suite 400

City Wakefield State MA Zip 01880

Telephone Day 719-395-2234 Evening _____ Fax _____ Pager/Cellular _____

Contact Name Patty Brooks

Policy Type Commercial General Liability

Policy Amount $5,000,000

Policy Number Will be provide by 8/10/26

AFFIDAVIT OF APPLICANT

I certify that the information contained in the foregoing application is true and correct to the best of my knowledge and belief that I have read, understand and agree to abide by the rules and regulations governing the proposed Special Event under the Redlands Municipal Code and I understand that this application is made subject to the rules and regulations established by the City Council and/or the City Manager or the City Manager's designee. Applicant agrees to comply will all other requirements of the City, County, State, Federal Government, and any other applicable entity which may pertain to the use of the Event venue and the conduct of the Event. In the event that a possessory interest subject to property taxation is created by virtue of this use permit, I agree to pay all possessory interest taxes and the City shall not be liable for the payment of such taxes I further agree that the payment of any such taxes shall not reduce any consideration paid to the City pursuant to this use permit. I agree to abide by these rules, and further certify that I, on behalf of the Host Organization, am also authorized to commit that organization, and therefore agree to be financially responsible for any costs and fees that may be incurred by or on behalf of the Event to the City of Redlands.

Print Name of Applicant/Host Organization: Anna Skoien/Brooksee Inc

Title: Operations Lead

Signature: annaskoien

Date: 7/31/2026

Print Name of Professional Event Organizer: Anna Skoien/Brooksee Inc

Title: Operations Lead

Signature: annaskoien

Date: 7/31/2026

Event: REVEL Big Bear Date: 11/7/2026

PERMIT TO CLOSE STREET FOR SOCIAL EVENT(S)

Permission to close a street for an event is subject to the following requirements:

1.	**Street Closure Diagram MUST be attached. (Failure to submit diagram will result in non-issuance of permit).**
2.	**Event Flyer or Event Description MUST be attached. (Failure to submit flyer or event description will result in non-issuance of permit).**
3.	**Applicant MUST provide insurance coverage per City's requirements (see reverse)**
4.	Written permission from all residents of the effected portion of the street MUST be attached.
5.	No tables or other objects shall be placed on the street surface.
6.	No alcohol shall be consumed on the street or City right-of-way outside of a permitted area.
7.	Temporary No Parking Signs and barricades shall be supplied and posted by City Staff
8.	Affected street(s) shall remain accessible for emergency vehicles and local traffic at all times.
9.	This permit pertains only to the closing of the street(s). This permit does not relate to the type of activity, noise, or any other aspect of the event. All other applicable and appropriate ordinances and laws apply.

Permission is hereby granted to: Brooksee Foundation/REVEL Big Bear

To close (street names) E San Bernardino Ave

Between (street names) Wabash Ave to Dearborn Street

Day & date 11/6/26 **Event times -** from (time) 7 ☑ am ☐ pm to (time) 5 ☐ am ☑ pm 11/7/26

Address of Applicant: 374 S 671 W Pleasant Grove, UT 84062 Phone No: 720-467-2188

Signature of Applicant: annaskoien Applicant Name (print): Anna Skoien

Condition(s); **set up & clean up time required:** The closure includes set up on Friday, November 6 at 7:00am through the event on Saturday, November 7 to 5:00pm

Event Description: Marathon and half marathon

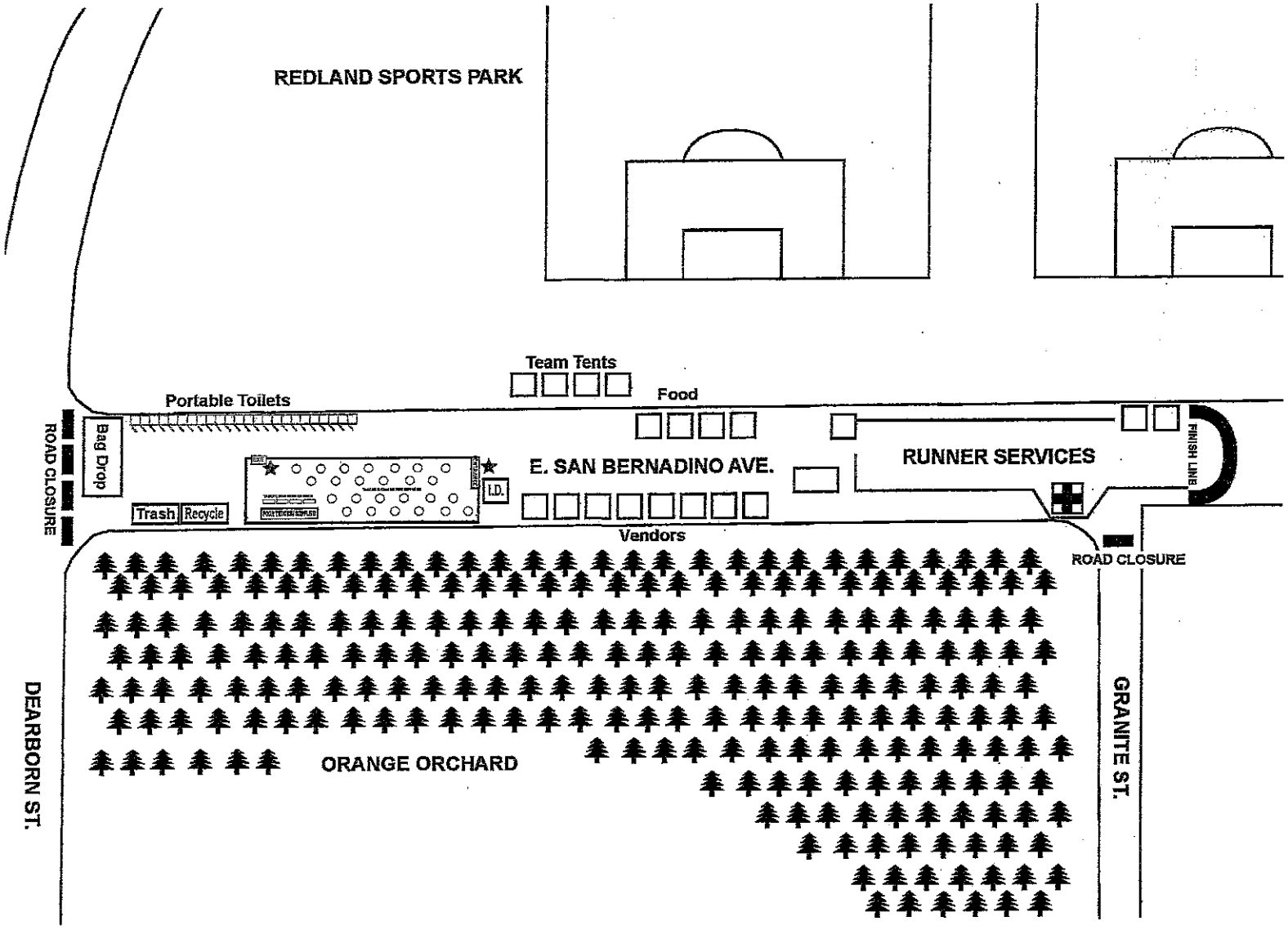
FOR OFFICE USE ONLY

This permit must be signed by the Chief of Police in order to be valid.

1. _____ Chief of Police — Date 8/13/26
2. _____ Municipal Utilities & Engineering Department — Date 8/20/26
3. _____ Facilities & Community Services Department — Date 8/11/26
4. _____ Risk Management Division — Date 8/20/26

Street Closure time: From 11/6/26 @ 7 ☒ am ☐ pm To 11/7/26 @ 7 ☐ am ☒ pm

Staff Notes:


REDLAND SPORTS PARK
Team Tents
Food
Portable Toilets
Bag Drop
ROAD CLOSURE
E. SAN BERNADINO AVE.
RUNNER SERVICES
FINISH LINE
Trash
Recycle
I.D.
Vendors
ROAD CLOSURE
DEARBORN ST.
ORANGE ORCHARD
GRANITE ST.

State of California

DAILY LICENSE APPLICATION

Department of Alcoholic Beverage Control

ABC USE ONLY		
License #	Receipt #	Fee $
Conditions Requested ☐ Yes ☐ No		Diagram Requested ☐ Yes ☐ No
License Type ☐ B & W ☐ General ☐ Special		

Complete all applicable items. Submit this application to your local ABC District Office with the required fee payable to ABC. To determine fee(s) due, visit https://www.abc.ca.gov/licensing/license-fees. Once the daily license is issued, fees cannot be refunded. Listing of ABC District Office is available at https://www.abc.ca.gov/contact/. Please visit https://www.abc.ca.gov/abc-221-instructions/ for further instructions.

SECTION 1. ORGANIZATION AND LICENSE TYPE INFORMATION

Organization Name	Tax ID
Brooksee Foundation	27-3405099
Organization Mailing Address	
374 S 671 W Pleasant Grove, UT 84062	

LICENSE TYPE

☑ Special Daily Beer and Wine
- ☐ Amateur Sports Organization
- ☐ Charitable
- ☐ Civic
- ☐ Cultural
- ☐ Fraternal
- ☐ Political
- ☐ Religious
- ☐ Social
- ☑ Other: 501c3 special event

☐ Daily General
- ☐ Political Party/Affiliate Supporting Candidate for Public Office or Ballot Measure
- ☐ Organization Formed for Specific Charitable or Civic Purpose
- ☐ Fraternal Organization in Existence over Five Years with Regular Membership
- ☐ Religious Organization
- ☐ Vessel per Section 24045.10 B&P ($50.00)

☐ Special Temporary License
- ☐ Television Station per Section 24045.2 or 24045.9 B&P
- ☐ Non-profit Corporation per Section 24045.4 and 24045.6 B&P
- ☐ Person conducting Estate Wine Sale per Section 24045.8 B&P
- ☐ Women's Educational and Charitable Organization per Section 24045.3 B&P
- ☐ Other Special Temporary License Per Section:

License #: Amount:

SECTION 2. EVENT DETAILS

Event Dates	Total # of Days	Hours of Alcoholic Beverage Sales, Service and/or consumption	Virtual Event
11/7/2026	1	7:00am To 1:00pm	☐ Yes ☑ No *Mark Yes, if the event is 100% virtual*

Event Address (Street #, name, and city)	Event Location Description (Jones Park, Pavilion A, etc.)	Location Within the City Limit
E San Bernardino Ave (Between Dearborn and Wabash)	**On E San Bernardino Ave by Redlands Sports Park**	☑ Yes ☐ No

Event Type	Type of Entertainment		Event Open to Public
☐Barbeque ☐Dinner ☑Sporting Event ☐Birthday ☐Festival ☐Social Gathering ☐Concert ☐Lunch ☐Wedding ☐Carnival ☐Mixer ☐Other: ☐Dance ☐Picnic			☑ Yes ☐ No
	Estimated Attendance	Security Guard If Yes, how many	Outdoor Event
	3000	☐Yes ☐No	☑ Yes* ☐ No **If Yes, a diagram of the event area is required*

REQUIRED

☑ By checking this box, you are certifying that you understand the requirements detailed in Business and Professions (B&P) Code Section 25682(c) which state that a nonprofit organization that has obtained a temporary daily license from the department must designate a person(s) to receive RBS training certification prior to the event, and that designated person(s) shall remain onsite for the duration of the event.

SECTION 3. CONTACT INFORMATION

Contact Person	Phone Number	Email Address
Anna Skoien	720-467-2188	anna@brooksee.com

SECTION 4. SIGNATURES AND APPROVALS

I attest that I am authorized by the organization named above to make this application on its behalf.

Organization's Authorized Representative Name	Phone Number	Signature	Date Signed
Anna Skoien	720-467-2188	annaSkoien	8/5/2026
Property Owner Approval By (Name) Required	Phone Number	Signature	Date Signed
Tabitha Crocker	909 798 7655	[signature]	8/10/26
Law Enforcement Approval By (Name), If applicable	Phone Number	Signature	Date Signed
Ryan Stemmons	909 647 8165	[signature]	8/12/26
District Office Approval By (Name)	Phone Number	ABC Employee Signature	Issuance Date

The above named organization is hereby licensed, pursuant to the California B&P Code Division 9 and California Code of Regulations, to engage in the temporary sale of alcoholic beverages for consumption at the abovenamed location for the period authorized above. B&P Code Section 25682(c) requires that a designated RBS-trained person(s) shall remain on site for the duration of the event. Failure to comply with this requirement will result in immediate cancellation of the permit. **This license may be revoked summarily by the Department if, in the opinion of the Department and/or the local law enforcement agency, it is necessary to protect the safety, welfare, health, peace and morals of the people of the State.**

Department of Alcoholic Beverage Control

State of California
Gavin Newsom, Governor

SUPPLEMENTAL DIAGRAM

Instructions to Applicant:
Draw a sketch of the area on which the licensed premises is or will be located Show adjacent structures and nearest cross streets. *If this is an event for a daily license, catering authorization, event authorization or miscellaneous use, show the area where sales and consumption of alcoholic beverages will occur. Post a copy of this diagram with Daily License, Catering Authorization or Event Authorization where the event is held. Sales and consumption of alcoholic beverages must be confined to the area designated in the diagram and supervised to prevent violations of the Alcoholic Beverage Control Act.*

1. APPLICANT NAME (Last, first, middle)	2. LICENSE TYPE
Skoien, Anna, Carrigan	Day License
3. PREMISES ADDRESS (Street number and name, city, zip code)	**4. NEAREST CROSS STREET**
On San Bernardino between Dearborn and Granite	Dearborn/Granite

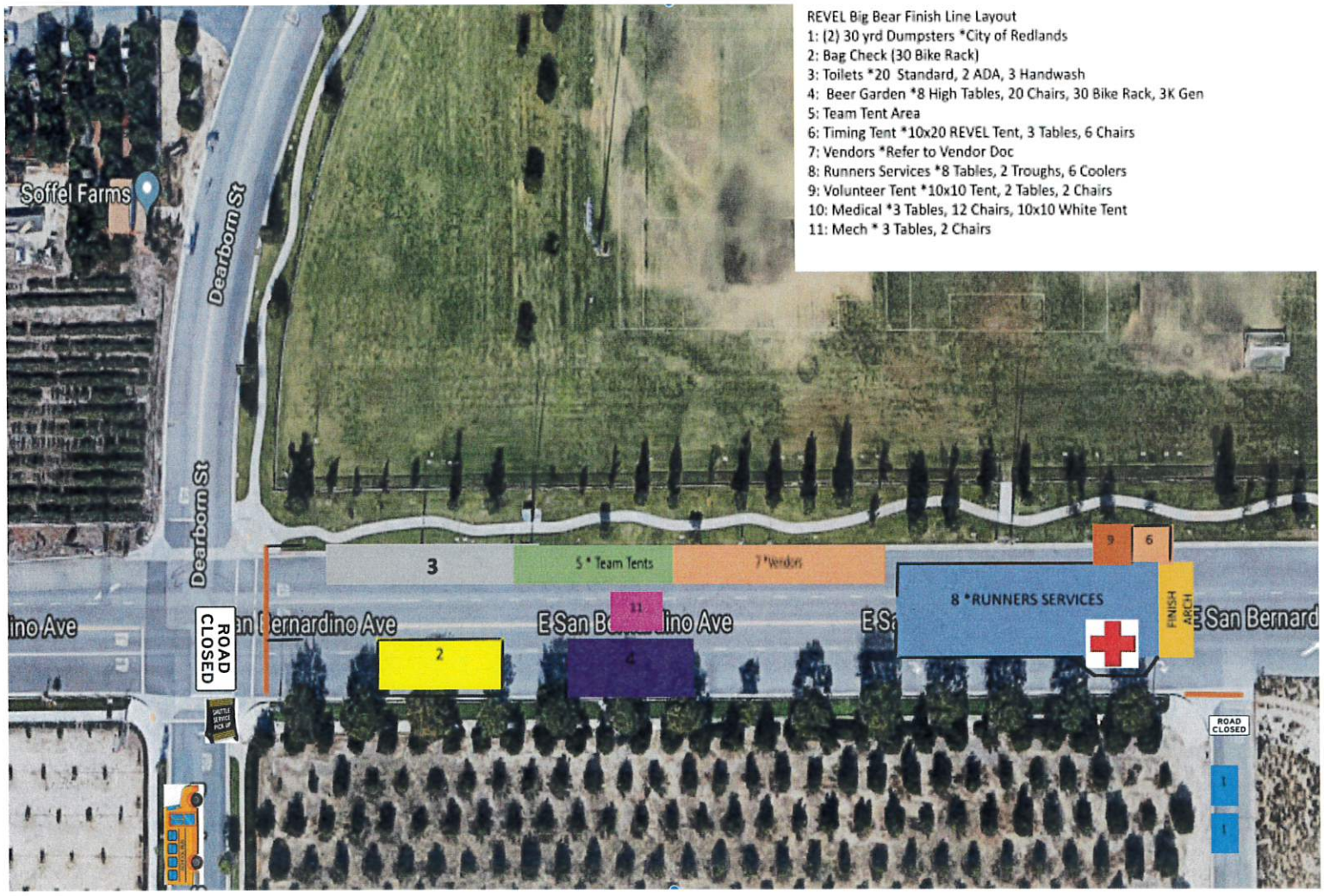
DIAGRAM

I have read the above instructions and I declare under penalty of perjury that the above diagram is true and correct.

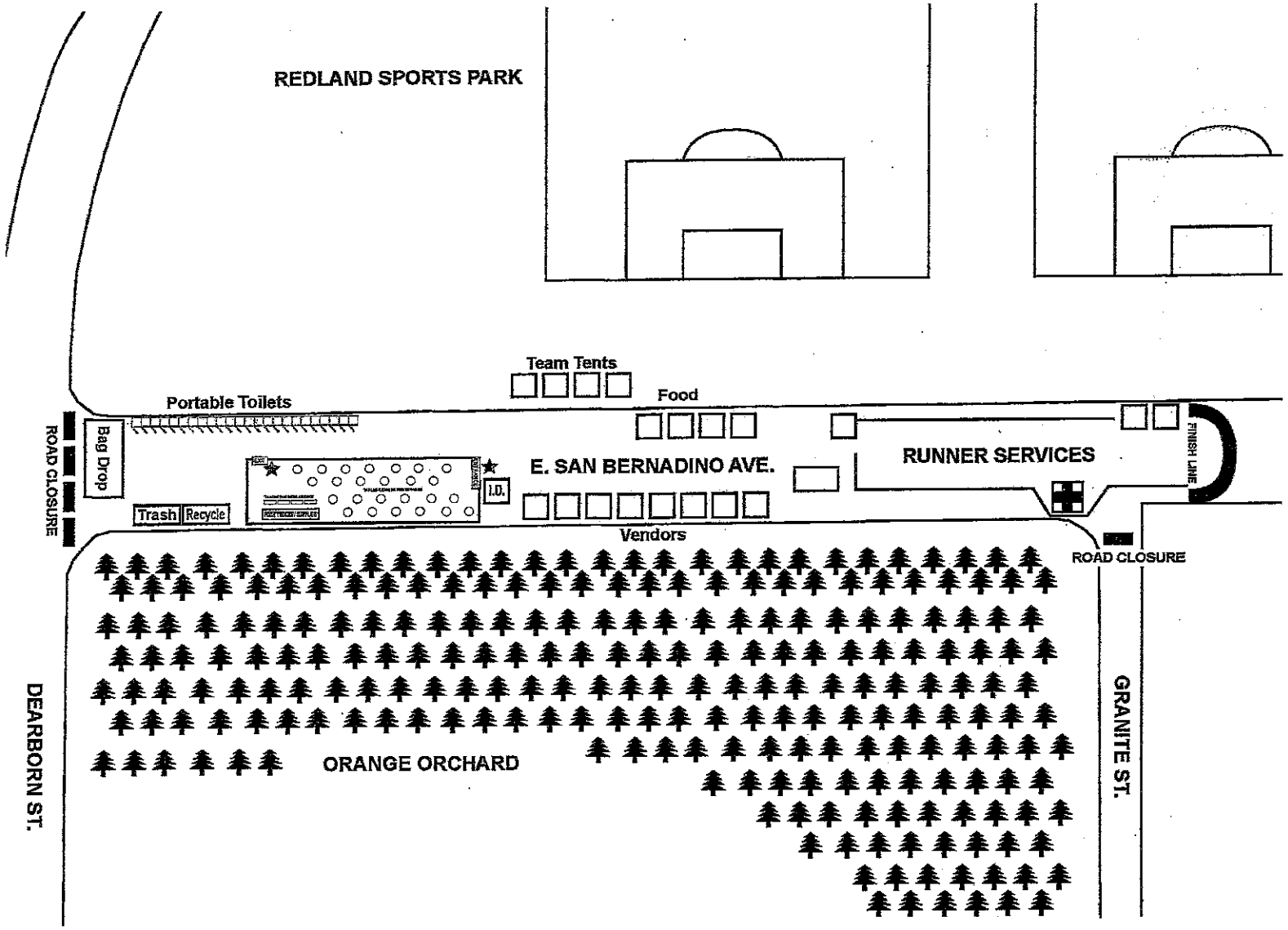
APPLICANT SIGNATURE	DATE SIGNED
Anna Skoien	8-5-2026

FOR ABC USE ONLY

CERTIFIED CORRECT (Signature)	PRINTED NAME	INSPECTION DATE



REVEL Big Bear Finish Line Layout
1: (2) 30 yrd Dumpsters *City of Redlands
2: Bag Check (30 Bike Rack)
3: Toilets *20 Standard, 2 ADA, 3 Handwash
4: Beer Garden *8 High Tables, 20 Chairs, 30 Bike Rack, 3K Gen
5: Team Tent Area
6: Timing Tent *10x20 REVEL Tent, 3 Tables, 6 Chairs
7: Vendors *Refer to Vendor Doc
8: Runners Services *8 Tables, 2 Troughs, 6 Coolers
9: Volunteer Tent *10x10 Tent, 2 Tables, 2 Chairs
10: Medical *3 Tables, 12 Chairs, 10x10 White Tent
11: Mech * 3 Tables, 2 Chairs


REDLAND SPORTS PARK
Team Tents
Food
Portable Toilets
Bag Drop
ROAD CLOSURE
E. SAN BERNADINO AVE.
RUNNER SERVICES
FINISH LINE
I.D.
Trash
Recycle
Vendors
ROAD CLOSURE
DEARBORN ST.
ORANGE ORCHARD
GRANITE ST.

INTERNAL REVENUE SERVICE
P. O. BOX 2508
CINCINNATI, OH 45201

DEPARTMENT OF THE TREASURY

Date: FEB 17 2016

BROOKSEE FOUNDATION
11968 ITHICA DR
HIGHLAND, UT 84003-0000

Employer Identification Number:

DLN:
26053442001956
Contact Person:
CUSTOMER SERVICE ID# 31954
Contact Telephone Number:
(877) 829-5500
Accounting Period Ending:
December 31
Public Charity Status:
509(a)(2)
Form 990/990-EZ/990-N Required:
Yes
Effective Date of Exemption:
February 9, 2016
Contribution Deductibility:
Yes
Addendum Applies:
No

Dear Applicant:

We're pleased to tell you we determined you're exempt from federal income tax under Internal Revenue Code (IRC) Section 501(c)(3). Donors can deduct contributions they make to you under IRC Section 170. You're also qualified to receive tax deductible bequests, devises, transfers or gifts under Section 2055, 2106, or 2522. This letter could help resolve questions on your exempt status. Please keep it for your records.

Organizations exempt under IRC Section 501(c)(3) are further classified as either public charities or private foundations. We determined you're a public charity under the IRC Section listed at the top of this letter.

If we indicated at the top of this letter that you're required to file Form 990/990-EZ/990-N, our records show you're required to file an annual information return (Form 990 or Form 990-EZ) or electronic notice (Form 990-N, the e-Postcard). If you don't file a required return or notice for three consecutive years, your exempt status will be automatically revoked.

If we indicated at the top of this letter that an addendum applies, the enclosed addendum is an integral part of this letter.

For important information about your responsibilities as a tax-exempt organization, go to www.irs.gov/charities. Enter "4221-PC" in the search bar to view Publication 4221-PC, Compliance Guide for 501(c)(3) Public Charities, which describes your recordkeeping, reporting, and disclosure requirements.

Sincerely,

Jeffrey I. Cooper
Director, Exempt Organizations
Rulings and Agreements

2026 REVEL Big Bear Comprehensive Operations Plan

Last updated: 08/3/2026

This document outlines the traffic control, safety, communication, and medical plan for the REVEL Big Bear Marathon & Half, to be held on Saturday, November 7, 2026. Brooksee's principal concern is the safety of our participants and of the public. As an organization, we wish to stress that we will take all necessary steps in order to ensure a safe event for all affected stakeholders.

Parking & Busing

All participants will park at an offsite, third-party private lot that will not require any special traffic control. Uniformed event staff members will be present to direct parking and ensure that safe conditions are maintained in the parking lots. We anticipate that participants will begin to arrive in the parking lot shortly before 3:30 AM See Exhibit A.

Participants will be loaded onto buses in the parking lots. Buses will be leaving from 3:15 AM to 3:45 AM to ensure that runners get to the starting lines before the 6:00 AM start time. Participants will not be allowed to park or be dropped off at the start venues.

Once participants finish the race, they will board shuttle buses at the finish line and be shuttled back to their vehicles at the parking area. See Exhibit A.

Course Routes

Course Route can be seen on our interactive Course Map page online.

The half marathon will start at 6:00 AM on Valley of the Falls Dr., approximately 3/4-mile East of Hwy 38 and Valley of the Falls Dr. intersection. Participants will be staged on the South side of Valley of the Falls Dr. Runners will run West on Valley of the Falls Dr. to Hwy 38. They will continue on Hwy 38 until Opal Dr. They will turn right (North) on Opal Dr. They will continue on Opal Dr. until East San Bernardino Ave.

They will turn left (West), and continue on East San Bernardino Ave until they reach the finish line between Dearborn St and Wabash Ave.

The full marathon will also start at 6:00 AM on Hwy 38 at the entrance CODES School Outdoor Science. Participants will be staged in Mile High Pines Camps. Runners will run South on Hwy 38. Upon reaching the T intersection of Hwy 38 and Valley of the Falls Drive, the marathon runners will turn right (West) to continue running on Hwy 38. They will run on Hwy 38 until Opal Dr. They Will turn right (North) on Opal Dr. They will continue on Opal Dr. until East San Bernardino Ave. They will turn left (West), and continue on East San Bernardino Ave until they reach the finish line between Dearborn St and Wabash Ave.

Once the full marathon course reaches the half marathon course, the two courses follow the same route to the finish venue.

General Traffic Control Along Race Course

Brooksee will engage TMI traffic control company to oversee the creation of engineered traffic control plans as well as event-day logistics. General traffic control plans for the race course are outlined below:

Half Marathon Start Line: Buses will leave the parking lots from 3:45-4:30 AM and proceed East on Hwy 38 to the staging area which is approximately 1/2 of a mile east of the Valley of the Falls Dr/Hwy 38 intersection on Valley of the Falls Dr. Staff members will be present at that location to direct runners off the bus and into the staging area and will direct the half marathon buses to continue East on Valley of the Falls Dr., turn around just North of Canyon Drive. They will then take Valley of the Falls Dr/Hwy 38 to the finish line on East San Bernardino Ave. Multiple staff members will be present to direct the flow of bus traffic and ensure safe conditions for participants. Cones and caution tape or pedestrian fencing will line Valley of the Falls Dr. to keep runners off the road until the race begins. There will be two openings, controlled by staff members, so that runners exiting the buses can enter the staging area. Runners will not be allowed to park or be dropped off at the start venue. Five minutes before the race begins (5:25 AM), participants will enter Valley of the Falls Drive to the start line. See Exhibit B for the Half Marathon start area.

Full Marathon Start Line: Buses will leave the parking lots from 3:15-3:45 AM and proceed North on Hwy 38 to the staging area. A race staff member will be present at that location to direct runners off the bus and into CODES/Mile High Pines Camp and will direct the full marathon buses to continue North on Hwy 38 to Hwy 18 and back to the finish staging area. Staff members will be present to direct the flow of bus traffic and ensure safe conditions for participants. Runners will not be allowed to park or be dropped off at the start venue. See Exhibit C. Five minutes prior to the start of the race (5:25 AM), participants will line up at the start line waiting for the race to begin.

- Highway 38 (CODES School of Outdoor Science to Valley of the Falls Dr/MP 4.95)
    - From 6:00 AM to 10:00 AM the Southbound lane will be closed to vehicular traffic. Cones will be placed on the double yellow lines. Officers will be staged at CODES as well as access points on Hwy 38 from CODES to the Valley of the Falls Dr. intersection. They will detour all traffic North of Angelus Oaks turning Southbound onto Hwy 38 to turn Northbound through Big Bear. The runners will enter the stretch at 6:25 AM. A pilot car system run by TMI will be escorting Angelus Oaks residents down the mountain in the Northbound Lane.
    - The Southbound lane will be closed from 6:00 AM to 10:00 AM. *PLEASE NOTE: The pilot car operation will be in effect from 6:00 AM to 10:00 AM.
- Valley of the Falls Drive (.7 miles East of Hwy 38) to the Valley of the Falls Dr. and Hwy 38 Intersection
    - Half marathon runners will start on Valley of the Falls Drive running west toward Hwy 38. From 6:00 AM to 6:15 AM officers will hold East and Westbound traffic on Valley of the Falls Dr. Runners will occupy both lanes on Valley of the Falls Drive until they reach the intersection of Valley of the Falls Dr. and Hwy 38
- Highway 38 - valley of the Falls Dr/MP 4.95 to MP 9.50
    - Starting at the intersection of Hwy 38 and Valley of the Falls Dr. to MP 9.50 half marathon runners will occupy the shoulder and the westbound lane from 6:00 to 6:45AM. A line of cones will be placed on the westbound shoulder line, and another line of cones will be placed down the center line. From 6:00 AM to 6:45 AM Westbound vehicles will be held in 15 min intervals at Valley of the Falls Dr. and Hwy 38. At 6:00 AM one CI--IP officer will take the first train of vehicles Westbound to the Pilot car system that begins at MP 9.50. He will then continue to his post in Redlands. Beginning at 6:30 AM, TMI pilot cars will take the waiting Westbound traffic to the Pilot car system. They will travel in the Eastbound lane until reaching the officer at MP 9.5. If needed, TMI will use the Westbound lane and travel slowly behind/alongside runners. This process will repeat itself every fifteen minutes until 6:45 AM.
    - Beginning at 7:15 AM, all half marathon runners still on this stretch (if any) will be instructed to vacate the westbound lane and run on the shoulder of Hwy 38 until they reach the pilot car system at MP 9.5.
    - All full marathon runners will remain in the westbound shoulder only (no lane encroachment) once they reach the Valley of the Falls Dr intersection. The CHP officer stationed at that intersection will verbally remind the full marathon runners to remain in the shoulder rather than the westbound lane beginning at that point.
    - Runners will be in this stretch from 6:00 AM to 11:00 AM.
- MP 9.50 (Marathon Mile 19) to Hwy 38 and Garnet St
    - Starting MP 9.50, the Westbound side of the road will be closed to vehicular traffic. Cones will be placed on the double yellow lines. A pilot escort operation will be deployed in the Eastbound lane. Officers will be staged at MP 9.50 and Hwy 38 and Garnet street for pilot car operation. For approximately four miles, runners will occupy

the entire Westbound lane. The lane will remain a full closure until the shoulder widens at Garnet St.
    - *PLEASE NOTE: The pilot car operation will be in effect from 6:00 AM to 12:00 PM. Their staging point will be MP 9.50 and the intersection of Garnet St and 38. The slowest runner will be through the pilot car stretch by 12:00 PM.
- Garnet St to Opal Ave
    - The Runners will then occupy the shoulder and lane encroachment equal to 12 feet of paved surface until turning right (North) on Opal Ave. While the runners are on the shoulder and encroachment, East and Westbound traffic will be open. Cones will be placed 12 feet from the Westbound paved edge to separate runners from traffic, and a separate line of delineators will be placed in the middle of the road creating an East and a Westbound lane.
    - Runners will be in this stretch from 7:00 AM and 11:00 PM.
- Opal Ave
    - From 7:05 AM to 12:32 PM runners will occupy the Western most side of the road (Southbound Traffic), up to 12 feet of paved surface. Cones will be placed 10-12 feet from the Southbound paved edge to separate runners from traffic, and a separate line of delineators will be placed in the middle of the road creating a North and Southbound lane.
    - TMI will close the Northbound lane of Opal Ave from Nice Ave to Hwy 38. This will help eliminate Northbound acceleration lane traffic from crossing the runners path as they cross Opal on Hwy 38. Closure will start from 6:50 AM to I PM .CHP will manage the intersection.
    - Runners will be in the section from 7:05 AM to 12:32 PM
- East San Bernardino Ave from Opal Ave to Wabash Ave.
    - From 7:00 AM to 1:00 PM runners will occupy the full Westbound lane. Cones will be placed on the center line to separate runners from Eastbound traffic. Eastbound Traffic will not be affected. Flaggers or staff will be placed at access points on the South side of E. San Bernardino Ave to ensure traffic only turns East. An officer will be stationed at Opal Ave and E. San Bernardino Ave to help runners turn West onto E. San Bernardino and to detour vehicles away from Westbound travel on E. San Bernardino Ave.
    - Runners will be in the section from 7:00 AM to 1:00 PM
- East San Bernardino Ave from Wabash Ave to Dearborn St.
    - East San Bernardino Ave will be closed to all traffic from Wabash Ave to Dearborn Street. Runners will occupy the full roadway, leaving 16 ft on the southernmost side of the road open for Emergency vehicles North and Southbound traffic will flow normally on Dearborn Ave as the closure will be on the east side of the intersection of Dearborn and San Bernardino.
    - For North and Southbound traffic on Wabash, on the south side of San Bernardino , they will have access to all roads, homes and Businesses without officer support . Upon reaching East San Bernardino Ave, vehicles will not be able to head Eastbound across San Bernardino without officer support.

- Vehicles heading Southbound on Wabash from the north side of E. San Bernardino Ave will also have to wait for officer support to either cross E San Bernardino to continue on Wabash or to turn East to drive in the one-way lane on E. San Bernardino Ave.

SAG Wagon: To ensure that the time frames listed above are adhered to, a sag wagon (escort vehicle) will collect all participants who are unable to maintain a pace of 15:00 per mile. This sag wagon will escort participants to the finish venue. Official race rules listed on our website indicate to all participants that if they are not able to maintain the 15:00 per mile pace, they must leave the route. See Exhibit D for a timetable that indicates where participants will be at specific times.

Resident & Business Notification

In the weeks leading up to the event, all residents and businesses located in the surrounding areas will receive an EDDM (Every Door Direct Mailer) postcard in the mail. This mailer explains all traffic control plans, delays, and other issues in relation to the event. It also lists our contact information and invites the public to reach out with questions or concerns.

In addition, we plan to partner with the local Chambers of Commerce to ensure that all businesses know what impacts to expect on race day, and give them an opportunity to get financial benefits from the event.

Participant Medical Plan

Aid stations will be established approximately every two miles along the entire race route, beginning near mile 3 of the full marathon. See Exhibit E for a sample aid station layout. Aid stations will be located on large shoulders and/or turnoff points adjacent to the runner lane to not obstruct the highway.

The locations of the 13 aid stations will be as follows:'

- Aid Station A: (34.1666449329, -116.90499592700002)
- Aid Station B: (34.1592566256, -116.92999679799999
- Aid Station C: (34.1571858305, -116.95978004699998)
- Aid Station D: (34.1486246735, -116.98101777800002)
- Aid Station E: (34.1230714425, -116.98259759899997)
- Aid Station F: (34.1019214686, -116.9664507)
- Aid Station G: (34.0985233003, -116.97731364700002)
- Aid Station H: (34.1036529021, -117.009672954)
- Aid Station 1: (34.0898264522, -117.03809095899999)
- Aid Station J: (34.0759345358, -117.06454826800001)
- Aid Station K: (34.07171008252401, -117.09906634676963)
- Aid Station L: (34.06990131660901, -117.11460633514719)
- Aid Station M: (34.0701161201, -117.13171346399997)

Volunteers manning each aid station will be carpooling to the area in 2-3 vehicles, and we have selected locations that allow for adequate room for them to park on the shoulders and/or pull outs next to the aid stations.

Each aid station, consisting of multiple portable tables and chairs, will be manned by several event staff. Staff members, who will be identified by matching event shirts, will ensure that runners are able to get proper nutrition and hydration when needed. All aid stations will be supplied with adequate water and electrolytes. These fluids will be delivered the day before the race in I-gallon jugs. The morning of the race, volunteers will pour the water and electrolytes into 5-gallon plastic coolers. The fluids will then be dispensed into 8-ounce waxed paper cups to be distributed to runners as they pass the aid stations.
Select aid stations will be supplied with other amenities such as energy bars and gels. In planning supplies for nutrition and hydration, we will plan our quantities based on the maximum possible intake per runner, and then add a contingency surplus to ensure that the risk of dehydration and exhaustion is minimized. In addition to aid stations along the route, water tables will also be set up at each starting line.

Each aid station along the route will be equipped with first aid kits. Event staff will be instructed concerning the use of these first aid kits. In addition, select aid stations (Aid Stations D, G, & K) will be accompanied by Prevent Medical staff. They will be capable of assisting participants with serious issues and/or emergencies.

In case of extreme cold weather, participants will be supplied with gloves and heating blankets to be used at the starting venues and during the race if desired. If at any point a participant is incapable of continuing down the canyon, they may elect to be picked up by the rear sag wagon and escorted down the route.

See Exhibit E for a sample aid station layout.

A large medical area will be established at the finish venue, adjacent to the finish line. This medical area will be staffed by several EMTs and other medical staff from Prevent Medical Services and American Medical Response. They will be equipped with all necessary medical supplies, including emergency supplies. In addition, an ALS ambulance will be on hand at the finish venue and will have unrestricted access to outside roads if it becomes necessary to transport any participants.

In addition to the ambulance stationed at the finish venue, an additional ALS ambulance (provided by AMR) will be stationed along the route. Both of these will constantly roam the route. There will also be 2 UTV's on course with medical personnel and EMT's that will roam and be able to respond quickly to any potential issues.

Communications Plan

A command post will be established at the finish venue to ensure that pertinent race information can be shared at all times with race staff and local authorities. Brooksee invites any and all law enforcement and government agencies related to the event to station a staff member at the command post.

Race staff will be using cell phones for communication during the event. Every aid station along the course will be equipped with a communication device so that pertinent information may be relayed to command. A communications list will be printed and distributed to each staff member; this list will identify the communication person that will be stationed at each aid station as well as at those fulfilling other roles during the event.

All event-related EMS vehicles stationed along the route will also be equipped with communication devices (radios or cell phones depending on their location).

Sanitation Plan

Portable restrooms will be set up in conjunction with each aid station along the route (every two miles) as well as at both starting lines and the finish venue. They will be delivered the day before the race and removed immediately following the race. Restroom quantities in all cases will be determined based upon usage estimates from the supplying company, which will always adhere to health code requirements, plus a safety surplus. Final numbers will not be determined until race management gains a solid estimate of how many participants will compete in the race. However, it is anticipated that each aid station will have roughly five to eight, and each start line will have roughly thirty to forty.

Abundant trash bins will be located at both starting lines, each aid station, and at multiple locations at the finish venue. Each location will be equipped with several extra industrial trash bags per bin. Event staff will be present at each aid station, the finish line, and both starting lines to ensure that trash bins remain accessible and that trash bags are changed when necessary.

Immediately following the start of the event, hired clean-up truck crews will begin to remove all trash and other items (including aid station tables and supplies and course signage) from the race route. Trash will be removed entirely from the canyon and taken to the finish venue, where roll-away dumpsters will be filled and hauled to the local landfill. Our aim is to leave no trace whatsoever of our event. Trash from each aid station will be loaded directly into the clean-up trucks along the route. Thus, no dumpsters will be necessary at the start venues nor along the course.

Insurance

Brooksee shall obtain a $5,000,000 insurance policy which covers every participant and volunteer associated with this event through the HCC Specialty.

Race Day Schedule

SATURDAY 11/7/2026

- 2:00: TMI begins to set up barricades on course
- 2:30am: Staff leaves for start lines/course
- 3:15-3:45am: Marathon Bus Loading @ 650 E Hospitality Lane, San Bernardino
- 3:30-4:15am: Half Marathon Bus Loading @ 650 E Hospitality Lane, San Bernardino
- 6:00am: Marathon (CODES) and Half Marathon Starts (Forest Falls)
- 6:00am: Security exchange at finish line (2@beer garden, 2@ finish line, 2 roving patrol)
- 7:15am: First Half Marathon runner arrives
- 8:20am: First Marathon runner arrives
- 8:00am - 1:00pm: Post-race shuttles operate

- 12:33pm: Course closes/last runner crosses finish line
- 1:00pm: Check course
- 2:30pm: Busing/parking lot cleanup
- 1:00-5:00pm: Finish line teardown/clean up
- 5:00pm: E San Bernardino reopens to traffic.

Contact Information

Operations Lead:

Anna Skoien: 720-467-2188

Exhibit A
Finish Venue Layout/Parking & Busing Map

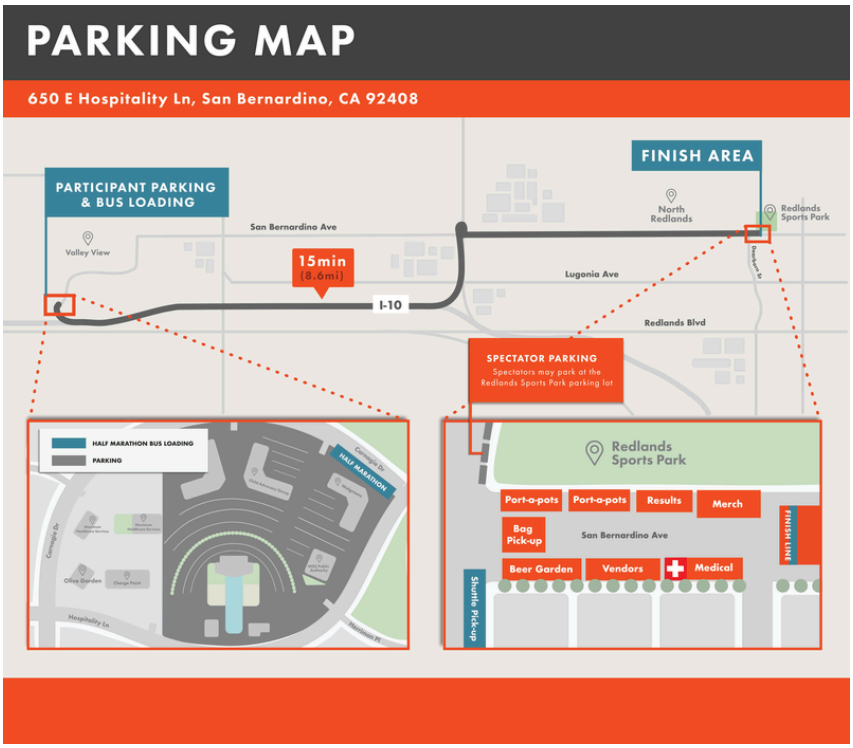


Exhibit B

Half Marathon Start Area

This area will be pedestrian fencing or cones w/caution tape. In two locations there will be 5-foot openings allowing runners to exit the shuttle and enter the staging area. These entrance points will be monitored by staff to ensure runners stay off the road and in the staging area.

Toilets for participants

Exhibit C

Full Marathon Start Area

Toilets for participants

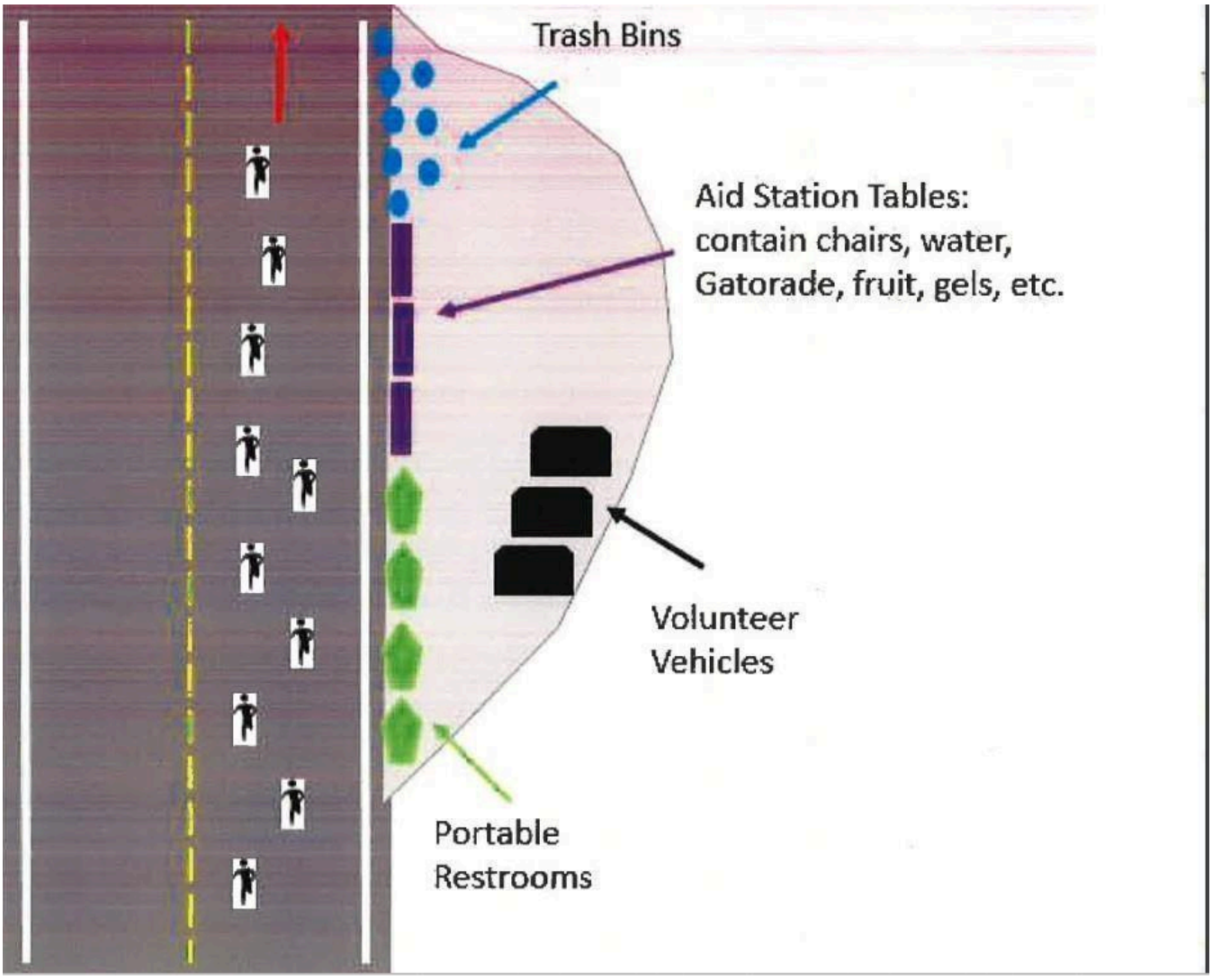
Runners will be staged in the parking lot away from the road. Prior to the race starting, staff will instruct the runners to line up at the start line.

Exhibit D

Mile	Landmark	First Runner Arrives	Last Runner Passes
1	Barton Flats Campground	6:05 AM	6:15 AM
2	N. Hathaway Road	6:11 AM	6:30 AM
3		6:30 AM	7:00 AM
4	Forest Road IN86	6:52 AM	7:30 AM
5		6:57 AM	7:45 AM
6		7:03 AM	8:00 AM
7		7•WAM	8:15 AM
8		7:14 AM	8:30 AM
9	Angelus Oak Fire Station	7:19 AM	8:45 AM
10		7:25 AM	9:00 AM
11		7:30 AM	9:15 AM
12		7:36 AM	9:30 AM
13		6:30 AM	9:45 AM
14	Valley of the Falls Dr	6:05 AM	10:00 AM
15		6:30 AM	10:15 AM
16	Old Mill Creek Rd	6:46 AM	10:30 AM
17	KilKare Road	6:52 AM	10:45 AM
18		6:57 AM	11:00 AM
19		7:03 AM	11:15 AM
20	Mill Creek Visitors Center	7:08 AM	11:30 AM
21		7:14 AM	11:45 AM
22	Hillsdale Drive	7:19 AM	12:00 PM
23	Mountain View Lane	7:25 AM	12:15 PM
24		7:30 AM	12:30 PM
25	Opal Ave	7:36 AM	12:45 PM
26	Wabash Ave	7:41 AM	1:00 PM

Exhibit E

Example Aid Station Layout



RESOLUTION NO. 7559

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS APPROVING THE DEFINITIONS OF ENCLOSED PUBLIC AREAS IN PUBLIC PARKS AND RESCINDING RESOLUTION NO. 4932

WHEREAS, the City of Redlands Quality of Life Department maintains and operates a park system for the citizens of the community; and

WHEREAS, the People of the State of California have enacted Article XI, Section 7 of the California Constitution empowering cities to make and enforce within their limits all local police, sanitary and other ordinances not in conflict with general laws; and

WHEREAS, the Redlands Municipal Code, Section 12.44.270 does allow, through the permitting process, the consumption of alcoholic beverages or liquors in enclosed public areas in public parks.

NOW THEREFORE BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF REDLANDS as follows:

Section 1. The definitions of enclosed public areas in public parks attached hereto as Exhibit "A" is hereby approved by the City Council.

Section 2. Resolution No. 4932 of the City Council of the City of Redlands is hereby rescinded.

ADOPTED, SIGNED AND APPROVED this 1st day of September, 2015.

Paul Foster, Mayor

ATTEST:

Sam Irwin, City Clerk

I, Sam Irwin, City Clerk of the City of Redlands, hereby certify that the foregoing Resolution was duly adopted by the City Council at a regular meeting thereof, held on the 1st day of September 2015, by the following vote:

AYES: Councilmembers Harrison, Gilbreath, Barich, James; Mayor Foster
NOES: None
ABSTAIN: None
ABSENT: None

Sam Irwin, City Clerk

"Exhibit A"

DEFINITIONS OF ENCLOSED PUBLIC AREAS IN PUBLIC PARKS

The following definitions shall apply in the filing of a permit with the City when requesting alcoholic beverages and liquors be consumed in public parks in enclosed public areas:

1. Alcoholic Drink – Any spirituous, vinous, malt, or mixed liquors.
2. Public Park- as defined in Section 12.44.010 C of the Redlands Municipal Code
3. Permit – as defined in Section 12.44.010 D of the Redlands Municipal Code
4. Enclosed public area
    a. Theatre – An outdoor structure providing for visual and performing arts
        i. Redlands Bowl – that portion of the seating area and extending in a westerly direction to eight feet within the curb face of Grant Street; extending in an easterly direction to eight feet within the curb face of Eureka Street; extending in a southerly direction to the park property line and extending in a northerly direction to the park property line.

        ii. Avice Meeker Sewell Theatre – that portion of the seating area and extending to within 100 feet of said seating area.

City Council **AGENDA ITEM NO. I18.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Adopt Resolution No. 8835, Rescinding Resolution No. 8809, Reaffirming the levying of special taxes within the City of Redlands Community Facilities District No. 2004-1, and directing the San Bernardino County Auditor/Controller/Treasurer/Tax Collector to place the City of Redlands Community Facilities District No. 2004-1 Special Taxes on the Fiscal Year 2026-2027 Tax Roll (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motion is provided:

1. I move to adopt Resolution No. 8835 rescinding Resolution No. 8809 and reaffirming the levying of special taxes within the City of Redlands Community Facilities District No. 2004-1 and directing the San Bernardino County Auditor/Controller/ Treasurer/Tax Collector to place the City of Redlands Community Facilities District No. 2004-1 special taxes on the Fiscal Year 2026-27 Tax Roll.

RECOMMENDATION:

Staff recommends that the City Council adopt Resolution No. 8835 rescinding Resolution No. 8809, reaffirming and approving the levying of special taxes within the City of Redlands Community Facilities District No. 2004-1 for Fiscal Year 2026-27, directing the San Bernardino County Auditor-Controller/Treasurer/Tax Collector to place the special taxes of the Fiscal Year 2026-27 Tax Roll, and authorizing the total amount of the special taxes, including applicable County administrative and processing fees, to satisfy the County’s requirements for placement on the annual property tax roll.

DISCUSSION:

A public hearing was held on June 16, 2026, to consider the placement of special taxes on parcels within the City of Redlands Community Facilities District No. 2004-1 for the Fiscal Year 2026-27 property tax roll. Following the public hearing, the City Council adopted Resolution No. 8809 confirming the special taxes and authorizing the submission of the special taxes to the San Bernardino County Auditor-Controller/Treasurer/Tax Collector.

Subsequent to the City's submission of the resolution and special taxes, the San Bernardino County Auditor-Controller/Treasurer/Tax Collector reviewed the resolution and is requiring additional clarification before accepting the direct charge submission for placement on the Fiscal Year 2026-27 tax roll. Specifically, the County requires that the resolutions expressly identify the applicable Fiscal Year 2026-27 tax roll, explicitly direct the Auditor-Controller/Treasurer/Tax Collector to place the charges on that tax roll, and clearly authorize the total amount of the direct charges, including any applicable County administrative or processing fees.

Resolution No. 8835 rescinds and replaces Resolution No. 8809 solely to incorporate the County's required clarifications while reaffirming the City Council's previous findings and approval of the assessment and submission of the special taxes to the San Bernardino County Auditor-Controller/Treasurer/Tax Collector for placement of City of Redlands Community Facilities District No. 2004-1 assessments on the Fiscal Year 2026-27 property tax roll. The replacement resolution does not modify the Engineer's Report, the special taxes, the properties subject to the special taxes, or the determinations made by the City Council following the duly noticed public hearing held on June 16, 2026. Rather, it provides the additional language required by the County to allow the previously approved direct charges to be processed and placed on the Fiscal Year 2026-27 tax roll.

ALTERNATIVES:

The City Council can choose not to adopt this resolution and provide alternative direction to staff. Declining to adopt the resolution will prevent the special taxes from being placed on the San Bernardino County Tax for roll Fiscal Year 2026-27 and may impact services provided.

STRATEGIC PLAN:

Not applicable

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Jocelynn Butters, Sr. Admin Assistant

FISCAL IMPACT

Fiscal Year: FY 26/27

Revenue Generating: No

Amount: N/A

Budgeted Y/N: N/A

Account No.: N/A

Additional Appropriation Required: No

Discussion:

The special tax revenue and related expenses are included in the FY 26/27 budget.

Attachments

Attachments

Resolution_No_8835_CFD_Tax_Levy.pdf
Exhibit_A_to_Resolution.pdf
Exhibit_B_to_Resolution.pdf
Resolution_No_8809.pdf

RESOLUTION NO. 8835

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS RECINDING RESOLUTION NO. 8809, APPROVING LEVYING SPECIAL TAXES WITHIN CITY OF REDLANDS COMMUNITY FACILITIES DISTRICT NO. 2004-1, AND DIRECTING THE SAN BERNARDINO COUNTY AUDITOR-CONTROLLER/TREASURER/TAX COLLECTOR TO PLACE THE CITY OF REDLANDS COMMUNITY FACILITIES DISTRICT NO. 2004-1 SPECIAL TAXES ON THE FISCAL YEAR 2026-2027 TAX ROLL

WHEREAS, the City Council of the City of Redlands (the "City") has formed City of Redlands Community Facilities District No. 2004-1 (Tract Map No. 16408 – Centex Homes) and annexed Tract Map No. 16287 (Annexation No. 1), Tentative Tract Map No. 17253 (Annexation No. 3), Parcel Map No. 17353 (Annexation No. 4), CRA No. 826 (Annexation No. 5), Tract Map No. 16806 (Annexation No. 8), Parcel Map No. 18208 (Annexation No. 9), Parcel Map No. 19371 (Annexation No. 11), Tract Map No. 16465, Tract Map No. 16627, Tract Map No. 18979, Tract Map No. 19975 and Tract Map No. 20079 (Annexation No. 12), Tract Map No. 18882 (Annexation No. 13), Parcel Map No. 19496 (Annexation No. 14), Parcel Map No. 18536-1 (Annexation No. 15), Tract Map No. 18988 (Annexation No. 16), Tract Map No. 17022 (Annexation No. 17), Parcel Map No. 19465 (Annexation No. 18), Tract Map No. 19942 (Annexation No. 19), Tract Map No. 19956 (Annexation No. 20), Tract Map No. 20126 (Annexation No. 21), Parcel Map No. 19981 (Annexation No. 22), Parcel Map No. 18536 (Annexation No. 23), CUP No. 1129 (Annexation No. 24), Tract Map No. 20065 (Annexation No. 25), Tract Map No. 20257 (Annexation No. 26), Planned Development No. 4 (Annexation No. 27), and Tract Map No. 20473 (Annexation No. 28), and Tract Map No. 20336 (Annexation No. 29), and Tract Map No.20528 (Annexation No. 30) into the City of Redlands Community Facilities District No. 2004-1 (the "Community Facilities District"), under and pursuant to the Mello-Roos Community Facilities Act of 1982 (the "Act"); and

WHEREAS, the City Council, as the legislative body of the Community Facilities District, is authorized under the Act to levy special taxes (the "Special Taxes") to pay for the costs of certain facilities and to authorize the issuance of bonds secured by the Special Taxes under the Act; and

WHEREAS, the City Council, pursuant to Ordinance No. 2584, adopted by the City Council of the City on August 3, 2004, and Resolution No. 6481, adopted on May 2, 2006, authorized and levied the Special Taxes within the Community Facilities District; and

WHEREAS, Section 53340 of the Act provides that the legislative body of a community facilities district may provide, by resolution, for the levy of the special tax in the current year or future tax years at the same rate or at a lower rate than the rate provided by ordinance, if the resolution is adopted and a certified list of all parcels subject to the special tax levy including the amount of the tax to be levied on each parcel for the applicable tax year, is filed by the clerk or other official designated by the legislative body with the county auditor. ; and

WHEREAS, the City Council desires to levy the Special Taxes within the Community Facilities District for Fiscal Year 2026-2027;

WHEREAS, the City Council desires to rescind Resolution No. 8809 and adopt this Resolution solely to clarify the direction to the San Bernardino County Auditor

Controller/Treasurer/Tax Collector regarding placement of the previously confirmed Special Taxes within the Community Facilities District on the Fiscal Year 2026–2027 tax roll and to expressly authorize the total amount of the direct charges, including any applicable County administrative or processing fees, without modifying the special taxes or the determinations made following the public hearing held on July 7, 2026.

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Redlands as follows:

Section 1. Resolution No. 8809 is hereby rescinded in its entirety and replaced by this Resolution. The City Council hereby reaffirms and approves the Special Taxes and expressly directs the San Bernardino County Auditor Controller/Treasurer/Tax Collector to place the levying of Special Taxes within the Community Facilities District Fiscal Year 2026-2027.

Section 2. The City Council hereby levies the Special Taxes for the Fiscal Year 2026- 2027 at the applied rates, up to the maximum, and with respect to the parcels as set forth in Exhibit A and Exhibit B hereto; provided, however, that the City Manager or the Finance Director of the City is hereby authorized, prior to the submission to the San Bernardino County Auditor/Controller and upon consultation with the City's special tax consultant, Webb Municipal Finance, LLC (a) to make any necessary modifications to such Special Taxes to correct any errors, omissions or inconsistencies in the listing or categorization of parcels to be taxed (provided that any such modifications shall not result in an increase in the Special Tax applicable to any category of parcels), or (b) to lower such Special Tax rates to the extent such officer deems necessary upon receipt of the final pricing information. The City Clerk of the City is hereby authorized and directed to file with the San Bernardino County Auditor/Controller no later than August 10, 2026, a certified list of all parcels subject to the Special Tax levy including the amount of the Special Tax to be levied on each parcel for Fiscal Year 2026-2027.

Section 3. That the City Council hereby authorizes and directs the San Bernardino County Auditor-Controller/Treasurer/Tax Collector to place the Community Facilities District No. 1 Assessment for Fiscal Year 2026-2027, plus the San Bernardino County Direct Charge processing fee of $0.30 per parcel, on the current tax roll and collected in the same manner as ordinary property taxes.

Section 4. The City Clerk of the City of Redlands is hereby authorized and directed to send a certified copy of this resolution to the San Bernardino County Auditor Controller/Treasurer/Tax Collector, or officer holding the equivalent position of auditor, for the County of San Bernardino.

ADOPTED, SIGNED AND APPROVED this October 6th, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, hereby certify that the foregoing Resolution was duly adopted at a regular meeting thereof, held on the 6th day of October 2026, by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

_____
Jeanne Donaldson, City Clerk

Exhibit A – Annexation Levy Summary by Assessor's Parcel Number

Exhibit B – Annexation Listing with Maximum and Applied Rates

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
1	0174651010000	$1,953.13	Original
2	0174651020000	$1,953.13	
3	0174651030000	$1,953.13	
4	0174651040000	$1,953.13	
5	0174651050000	$1,953.13	
6	0174651060000	$1,953.13	
7	0174651070000	$1,953.13	
8	0174651080000	$1,953.13	
9	0174651090000	$1,953.13	
10	0174651100000	$1,953.13	
11	0174651110000	$1,953.13	
12	0174651120000	$1,953.13	
13	0174651130000	$1,953.13	
14	0174651140000	$1,953.13	
15	0174651150000	$1,953.13	
16	0174651160000	$1,953.13	
17	0174651170000	$1,953.13	
18	0174651180000	$1,953.13	
19	0174651190000	$1,953.13	
20	0174651200000	$1,953.13	
21	0174651210000	$1,953.13	
22	0174651220000	$1,953.13	
23	0174651230000	$1,953.13	
24	0174651240000	$1,953.13	
25	0174651250000	$1,953.13	
26	0174651260000	$1,953.13	
27	0174651270000	$1,953.13	
28	0174651280000	$1,953.13	
29	0174651290000	$1,953.13	
30	0174651300000	$1,953.13	
31	0174651310000	$1,953.13	
32	0174651320000	$1,953.13	
33	0174651330000	$1,953.13	
34	0174651340000	$1,953.13	
35	0174661010000	$1,953.13	
36	0174661020000	$1,953.13	
37	0174661030000	$1,953.13	
38	0174661040000	$1,953.13	
39	0174661050000	$1,953.13	
40	0174661060000	$1,953.13	
41	0174661070000	$1,953.13	
42	0174661080000	$1,953.13	
43	0174661090000	$1,953.13	
44	0174661100000	$1,953.13	
45	0174661110000	$1,953.13	
46	0174661120000	$1,953.13	
47	0174661130000	$1,953.13	
48	0174661140000	$1,953.13	
49	0174661150000	$1,953.13	
50	0174661160000	$1,953.13	
51	0174661170000	$1,953.13	
52	0174661180000	$1,953.13	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
53	0174661190000	$1,953.13	
54	0174661200000	$1,953.13	
55	0174661210000	$1,953.13	
56	0174661220000	$1,953.13	
57	0174661230000	$1,953.13	
58	0174661240000	$1,953.13	
59	0174661250000	$1,953.13	
60	0174661260000	$1,953.13	
61	0174661270000	$1,953.13	
62	0174661280000	$1,953.13	
63	0174661290000	$1,953.13	
64	0174661300000	$1,953.13	
65	1212371080000	$491.67	Annex No. 1
66	1212371090000	$491.67	
67	1212371100000	$491.67	
68	1212371110000	$491.67	
69	1212371120000	$491.67	
70	1212371130000	$491.67	
71	1212371140000	$491.67	
72	1212371150000	$491.67	
73	1212371160000	$491.67	
74	1212371170000	$491.67	
75	1212371180000	$491.67	
76	1212371190000	$491.67	
77	0174252200000	$4,324.13	Annex No. 4
78	0174691060000	$261.72	
79	0174691070000	$261.72	
80	0174691080000	$261.72	
81	0174691090000	$261.72	
82	0174691100000	$261.72	
83	0174691110000	$261.72	
84	0174691120000	$261.72	
85	0174691130000	$261.72	
86	0174691140000	$261.72	
87	0174691150000	$261.72	
88	0174691160000	$357.64	
89	0174691170000	$357.64	
90	0174691180000	$357.64	
91	0174691190000	$357.64	
92	0174691200000	$357.64	
93	0174691210000	$357.64	
94	0174691220000	$357.64	
95	0174691230000	$261.72	
96	0174691240000	$261.72	
97	0174691250000	$261.72	
98	0174691260000	$261.72	
99	0174691270000	$261.72	
100	0174691280000	$261.72	
101	0174691290000	$261.72	
102	0174691300000	$261.72	
103	0174691310000	$261.72	
104	0174691320000	$261.72	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
105	0174691330000	$284.49	
106	0174691340000	$284.49	
107	0174691350000	$284.49	
108	0174691360000	$284.49	
109	0292061490000	$7,080.84	Annex No. 5
110	0292061500000	$3,319.15	
111	0292631020000	$454.83	Annex No. 9
112	0292631030000	$454.83	
113	0292631040000	$454.83	
114	0292631050000	$454.83	
115	0292631060000	$454.83	
116	0292631070000	$454.83	
117	0292631080000	$454.83	
118	0292631090000	$454.83	
119	0292631100000	$454.83	
120	0292631110000	$454.83	
121	0292631120000	$454.83	
122	0292631130000	$454.83	
123	0292631140000	$454.83	
124	0292631150000	$454.83	
125	0292631160000	$454.83	
126	0292631170000	$454.83	
127	0292631180000	$454.83	
128	0292631190000	$454.83	
129	0292631200000	$454.83	
130	0292631210000	$454.83	
131	0292631220000	$454.83	
132	0292631230000	$454.83	
133	0292631240000	$454.83	
134	0292631250000	$454.83	
135	0292631260000	$454.83	
136	0292631270000	$454.83	
137	0292631280000	$454.83	
138	0292631290000	$454.83	
139	0292631300000	$454.83	
140	0292631310000	$454.83	
141	0292631320000	$454.83	
142	1212451010000	$1,052.46	Annex No. 12a
143	1212451020000	$1,052.46	
144	1212451030000	$1,052.46	
145	1212451040000	$1,052.46	
146	1212451050000	$1,052.46	
147	1212451060000	$1,052.46	
148	1212451070000	$1,052.46	
149	1212451080000	$1,052.46	
150	1212451090000	$1,052.46	
151	1212451100000	$1,052.46	
152	1212451110000	$1,052.46	
153	1212451120000	$1,052.46	
154	1212451130000	$1,052.46	
155	1212451140000	$1,052.46	
156	1212451150000	$1,052.46	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
157	1212451160000	$1,052.46	
158	1212451170000	$1,052.46	
159	1212451180000	$1,052.46	
160	1212451190000	$1,052.46	
161	1212451200000	$1,052.46	
162	1212451210000	$1,052.46	
163	1212451220000	$1,052.46	
164	1212451230000	$1,052.46	
165	1212451240000	$1,052.46	
166	1212451250000	$1,052.46	
167	1212451260000	$1,052.46	
168	1212451270000	$1,052.46	
169	1212451280000	$1,052.46	
170	1212451290000	$1,052.46	
171	1212451300000	$1,052.46	
172	1212451310000	$1,052.46	
173	1212451320000	$1,052.46	
174	1212451330000	$1,052.46	
175	1212451340000	$1,052.46	
176	1212451350000	$1,052.46	
177	1212451360000	$1,052.46	
178	1212451370000	$1,052.46	
179	1212451380000	$1,052.46	
180	1212451390000	$1,052.46	
181	1212451400000	$1,052.46	
182	1212451410000	$1,052.46	
183	1212451420000	$1,052.46	
184	1212451430000	$1,052.46	
185	1212451440000	$1,052.46	
186	1212451450000	$1,052.46	
187	1212451460000	$1,052.46	
188	1212451470000	$1,052.46	
189	1212451480000	$1,052.46	
190	1212451490000	$1,052.46	
191	1212451500000	$1,052.46	
192	1212451510000	$1,052.46	
193	1212451520000	$1,052.46	
194	1212451530000	$1,052.46	
195	1212451540000	$1,052.46	
196	1212451550000	$1,052.46	
197	1212451560000	$1,052.46	
198	1212451570000	$1,052.46	
199	1212451580000	$1,052.46	
200	1212451590000	$1,052.46	
201	1212451600000	$1,052.46	
202	1212451610000	$1,052.46	
203	0168891010000	$1,185.00	Annex. No. 12b
204	0168891020000	$1,185.00	
205	0168891030000	$1,185.00	
206	0168891040000	$1,185.00	
207	0168891050000	$1,185.00	
208	0168891060000	$1,185.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
209	0168891070000	$1,185.00	
210	0168891080000	$1,185.00	
211	0168891090000	$1,185.00	
212	0168891100000	$1,185.00	
213	0168891110000	$1,185.00	
214	0168891120000	$1,185.00	
215	0168891130000	$1,185.00	
216	0168891140000	$1,185.00	
217	0168891150000	$1,185.00	
218	0168891160000	$1,185.00	
219	0168891170000	$1,185.00	
220	0168891180000	$1,185.00	
221	0168891190000	$1,185.00	
222	0168891200000	$1,185.00	
223	0168071170000	$1,065.57	Annex. No. 12c
224	0168071180000	$1,065.57	
225	0168071190000	$1,065.57	
226	0168071200000	$1,065.57	
227	0168071210000	$1,065.57	
228	0168071220000	$1,065.57	
229	0168071230000	$1,065.57	
230	0168071240000	$1,065.57	
231	0168071250000	$1,065.57	
232	0168071260000	$1,065.57	
233	0168071270000	$1,065.57	
234	0168071280000	$1,065.57	
235	0168071290000	$1,065.57	
236	0168071300000	$1,065.57	
237	0168071310000	$1,065.57	
238	0168071320000	$1,065.57	
239	0168071330000	$1,065.57	
240	0168071340000	$1,065.57	
241	0168071350000	$1,065.57	
242	0168071360000	$1,065.57	
243	0168071370000	$1,065.57	
244	0168071380000	$1,065.57	
245	0168071390000	$1,065.57	
246	0168071400000	$1,065.57	
247	0168071410000	$1,065.57	
248	0168071420000	$1,065.57	
249	0168071430000	$1,065.57	
250	0168071440000	$1,065.57	
251	0168071450000	$1,065.57	
252	0168071460000	$1,065.57	
253	0168071470000	$1,065.57	
254	0168071480000	$1,065.57	
255	0168071490000	$1,065.57	
256	0168071500000	$1,065.57	
257	0168071510000	$1,065.57	
258	0168071520000	$1,065.57	
259	0168071530000	$1,065.57	
260	0168071540000	$1,065.57	
261	0168071550000	$1,065.57	
262	0168071560000	$1,065.57	
263	0168071570000	$1,065.57	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
264	0168071580000	$1,065.57
265	0168071590000	$1,065.57
266	0168071600000	$1,065.57
267	0168071610000	$1,065.57
268	0168071620000	$1,065.57
269	0168071630000	$1,065.57
270	0168071640000	$1,065.57
271	0168071650000	$1,065.57
272	0168071660000	$1,065.57
273	0168071670000	$1,065.57
274	0168071680000	$1,065.57
275	0168071690000	$1,065.57
276	0168071700000	$1,065.57
277	0168071710000	$1,065.57
278	0168901010000	$1,065.57
279	0168901020000	$1,065.57
280	0168901030000	$1,065.57
281	0168901040000	$1,065.57
282	0168901050000	$1,065.57
283	0168901060000	$1,065.57
284	0168901070000	$1,065.57
285	0168901080000	$1,065.57
286	0168901090000	$1,065.57
287	0168901100000	$1,065.57
288	0168901110000	$1,065.57
289	0168901120000	$1,065.57
290	0168901130000	$1,065.57
291	0168901140000	$1,065.57
292	0168901150000	$1,065.57
293	0168901160000	$1,065.57
294	0168901170000	$1,065.57
295	0168901180000	$1,065.57
296	0168901190000	$1,065.57
297	0168901200000	$1,065.57
298	0168901210000	$1,065.57
299	0168901220000	$1,065.57
300	0168901230000	$1,065.57
301	0168901240000	$1,065.57
302	0168901250000	$1,065.57
303	0168901260000	$1,065.57
304	0168901270000	$1,065.57
305	0168901280000	$1,065.57
306	0168901290000	$1,065.57
307	0168901300000	$1,065.57
308	0168901310000	$1,065.57
309	0168901320000	$1,065.57
310	0168901330000	$1,065.57
311	0168901340000	$1,065.57
312	0168901350000	$1,065.57
313	0168901360000	$1,065.57
314	0168901370000	$1,065.57
315	0168901380000	$1,065.57
316	0168901390000	$1,065.57
317	0168901400000	$1,065.57
318	0168901410000	$1,065.57

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
319	0168901420000	$1,065.57	
320	0168901430000	$1,065.57	
321	0168901440000	$1,065.57	
322	0168901450000	$1,065.57	
323	0168901460000	$1,065.57	
324	0168901470000	$1,065.57	
325	0168901480000	$1,065.57	
326	0168901490000	$1,065.57	
327	0168901500000	$1,065.57	
328	0168901510000	$1,065.57	
329	0168901520000	$1,065.57	
330	0168901530000	$1,065.57	
331	0168901540000	$1,065.57	
332	0168901550000	$1,065.57	
333	0168901560000	$1,065.57	
334	0168901570000	$1,065.57	
335	0168901580000	$1,065.57	
336	0168901590000	$1,065.57	
337	0168901600000	$1,065.57	
338	0168901610000	$1,065.57	
339	0168901620000	$1,065.57	
340	0168901630000	$1,065.57	
341	0168901640000	$1,065.57	
342	0168901650000	$1,065.57	
343	0168901660000	$1,065.57	
344	0168901670000	$1,065.57	
345	0168071760000	$1,071.43	Annex No. 12d
346	0168071770000	$1,071.43	
347	0168071780000	$1,071.43	
348	0168071790000	$1,071.43	
349	0168071800000	$1,071.43	
350	0168071810000	$1,071.43	
351	0168071820000	$1,071.43	
352	0168071830000	$1,071.43	
353	0168071840000	$1,071.43	
354	0168071850000	$1,071.43	
355	0168071860000	$1,071.43	
356	0168071870000	$1,071.43	
357	0168071880000	$1,071.43	
358	0168071890000	$1,071.43	
359	0292053160000	$10,000.08	Annex No. 14
360	0167422010000	$1,317.07	Annex No. 16
361	0167422020000	$1,317.07	
362	0167422030000	$1,317.07	
363	0167422040000	$1,317.07	
364	0167422050000	$1,317.07	
365	0167422060000	$1,317.07	
366	0167422070000	$1,317.07	
367	0167422080000	$1,317.07	
368	0167422090000	$1,317.07	
369	0167422100000	$1,317.07	
370	0167422110000	$1,317.07	
371	0167422120000	$1,317.07	
372	0167422130000	$1,317.07	
373	0167422140000	$1,317.07	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
374	0167422150000	$1,317.07
375	0167422160000	$1,317.07
376	0167422170000	$1,317.07
377	0167422180000	$1,317.07
378	0167422190000	$1,317.07
379	0167422200000	$1,317.07
380	0167422210000	$1,317.07
381	0167422220000	$1,317.07
382	0167422230000	$1,317.07
383	0167422240000	$1,317.07
384	0167422250000	$1,317.07
385	0167422260000	$1,317.07
386	0167422270000	$1,317.07
387	0167422280000	$1,317.07
388	0167422290000	$1,317.07
389	0167422300000	$1,317.07
390	0167422310000	$1,317.07
391	0167422320000	$1,317.07
392	0167422330000	$1,317.07
393	0167422340000	$1,317.07
394	0167422350000	$1,317.07
395	0167422360000	$1,317.07
396	0167422370000	$1,317.07
397	0167422380000	$1,317.07
398	0167422390000	$1,317.07
399	0167422400000	$1,317.07
400	0167422410000	$1,317.07
401	0167422420000	$1,317.07
402	0167432010000	$1,317.07
403	0167432020000	$1,317.07
404	0167432030000	$1,317.07
405	0167432040000	$1,317.07
406	0167432050000	$1,317.07
407	0167432060000	$1,317.07
408	0167432070000	$1,317.07
409	0167432080000	$1,317.07
410	0167432090000	$1,317.07
411	0167432100000	$1,317.07
412	0167432110000	$1,317.07
413	0167432120000	$1,317.07
414	0167432130000	$1,317.07
415	0167432140000	$1,317.07
416	0167432150000	$1,317.07
417	0167432160000	$1,317.07
418	0167432170000	$1,317.07
419	0167432180000	$1,317.07
420	0167432190000	$1,317.07
421	0167432200000	$1,317.07
422	0167432210000	$1,317.07
423	0167432220000	$1,317.07
424	0167432230000	$1,317.07
425	0167432240000	$1,317.07
426	0167432250000	$1,317.07
427	0167432260000	$1,317.07
428	0167432270000	$1,317.07

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
429	0167432280000	$1,317.07	
430	0167432290000	$1,317.07	
431	0167432300000	$1,317.07	
432	0167432310000	$1,317.07	
433	0167432320000	$1,317.07	
434	0167432330000	$1,317.07	
435	0167432340000	$1,317.07	
436	0167432350000	$1,317.07	
437	0167432360000	$1,317.07	
438	0167432370000	$1,317.07	
439	0167432380000	$1,317.07	
440	0167432390000	$1,317.07	
441	0167432400000	$1,317.07	
442	0299431010000	$1,352.94	Annex No. 19
443	0299431020000	$1,352.94	
444	0299431030000	$1,352.94	
445	0299431040000	$1,352.94	
446	0299431050000	$1,352.94	
447	0299431060000	$1,352.94	
448	0299431070000	$1,352.94	
449	0299431080000	$1,352.94	
450	0299431090000	$1,352.94	
451	0299431100000	$1,352.94	
452	0299431110000	$1,352.94	
453	0299431120000	$1,352.94	
454	0299431130000	$1,352.94	
455	0299431140000	$1,352.94	
456	0299431150000	$1,352.94	
457	0299431160000	$1,352.94	
458	0299431170000	$1,352.94	
459	0299431180000	$1,352.94	
460	0299431190000	$1,352.94	
461	0299431200000	$1,352.94	
462	0299431210000	$1,352.94	
463	0299431220000	$1,352.94	
464	0299431230000	$1,352.94	
465	0299431240000	$1,352.94	
466	0299431250000	$1,352.94	
467	0299431260000	$1,352.94	
468	0299431270000	$1,352.94	
469	0299431280000	$1,352.94	
470	0299431290000	$1,352.94	
471	0299431300000	$1,352.94	
472	0299431310000	$1,352.94	
473	0299431320000	$1,352.94	
474	0299431330000	$1,352.94	
475	0299431340000	$1,352.94	
476	0299421010000	$1,150.00	Annex No. 20
477	0299421020000	$1,150.00	
478	0299421030000	$1,150.00	
479	0299421040000	$1,150.00	
480	0299421050000	$1,150.00	
481	0299421060000	$1,150.00	
482	0299421070000	$1,150.00	
483	0299421080000	$1,150.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
484	0299421090000	$1,150.00	
485	0299421100000	$1,150.00	
486	0299421110000	$1,150.00	
487	0299421120000	$1,150.00	
488	0299421130000	$1,150.00	
489	0299421140000	$1,150.00	
490	0299421150000	$1,150.00	
491	0299421160000	$1,150.00	
492	0299421170000	$1,150.00	
493	0299421180000	$1,150.00	
494	0299421190000	$1,150.00	
495	0299421200000	$1,150.00	
496	0299421210000	$1,150.00	
497	0299421220000	$1,150.00	
498	0299421230000	$1,150.00	
499	0299421240000	$1,150.00	
500	0299421250000	$1,150.00	
501	0299421260000	$1,150.00	
502	0299421270000	$1,150.00	
503	0299421280000	$1,150.00	
504	0299421290000	$1,150.00	
505	0299421300000	$1,150.00	
506	0299421310000	$1,150.00	
507	0299421320000	$1,150.00	
508	0299421330000	$1,150.00	
509	0299421340000	$1,150.00	
510	0299421350000	$1,150.00	
511	0299421360000	$1,150.00	
512	0299421370000	$1,150.00	
513	0299421380000	$1,150.00	
514	0299421390000	$1,150.00	
515	0299421400000	$1,150.00	
516	0168911010000	$1,380.95	Annex No. 21
517	0168911020000	$1,380.95	
518	0168911030000	$1,380.95	
519	0168911040000	$1,380.95	
520	0168911050000	$1,380.95	
521	0168911060000	$1,380.95	
522	0168911070000	$1,380.95	
523	0168911080000	$1,380.95	
524	0168911090000	$1,380.95	
525	0168911100000	$1,380.95	
526	0168911110000	$1,380.95	
527	0168911120000	$1,380.95	
528	0168911130000	$1,380.95	
529	0168911140000	$1,380.95	
530	0168911150000	$1,380.95	
531	0168911160000	$1,380.95	
532	0168911170000	$1,380.95	
533	0168911180000	$1,380.95	
534	0168911190000	$1,380.95	
535	0168911200000	$1,380.95	
536	0168911210000	$1,380.95	
537	0168911220000	$1,380.95	
538	0168911230000	$1,380.95	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
539	0168911240000	$1,380.95
540	0168911250000	$1,380.95
541	0168911260000	$1,380.95
542	0168911270000	$1,380.95
543	0168911280000	$1,380.95
544	0168911290000	$1,380.95
545	0168911300000	$1,380.95
546	0168911310000	$1,380.95
547	0168911320000	$1,380.95
548	0168911330000	$1,380.95
549	0168911340000	$1,380.95
550	0168911350000	$1,380.95
551	0168911360000	$1,380.95
552	0168911370000	$1,380.95
553	0168911380000	$1,380.95
554	0168911390000	$1,380.95
555	0168911400000	$1,380.95
556	0168911410000	$1,380.95
557	0168911420000	$1,380.95
558	0168911430000	$1,380.95
559	0168911440000	$1,380.95
560	0168911450000	$1,380.95
561	0168911460000	$1,380.95
562	0168911470000	$1,380.95
563	0168911480000	$1,380.95
564	0168911490000	$1,380.95
565	0168911500000	$1,380.95
566	0168911510000	$1,380.95
567	0168911520000	$1,380.95
568	0168921010000	$1,380.95
569	0168921020000	$1,380.95
570	0168921030000	$1,380.95
571	0168921040000	$1,380.95
572	0168921050000	$1,380.95
573	0168921060000	$1,380.95
574	0168921070000	$1,380.95
575	0168921080000	$1,380.95
576	0168921090000	$1,380.95
577	0168921100000	$1,380.95
578	0168921110000	$1,380.95
579	0168921120000	$1,380.95
580	0168921130000	$1,380.95
581	0168921140000	$1,380.95
582	0168921150000	$1,380.95
583	0168921160000	$1,380.95
584	0168921170000	$1,380.95
585	0168921180000	$1,380.95
586	0168921190000	$1,380.95
587	0168921200000	$1,380.95
588	0168921210000	$1,380.95
589	0168921220000	$1,380.95
590	0168921230000	$1,380.95
591	0168921240000	$1,380.95
592	0168921250000	$1,380.95
593	0168921260000	$1,380.95

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
594	0168921270000	$1,380.95	
595	0168921280000	$1,380.95	
596	0168921290000	$1,380.95	
597	0168921300000	$1,380.95	
598	0168921310000	$1,380.95	
599	0168921320000	$1,380.95	
600	0168921330000	$1,380.95	
601	0168921340000	$1,380.95	
602	0168921350000	$1,380.95	
603	0168921360000	$1,380.95	
604	0168921370000	$1,380.95	
605	0168921380000	$1,380.95	
606	0168921390000	$1,380.95	
607	0168921400000	$1,380.95	
608	0168921410000	$1,380.95	
609	0168921420000	$1,380.95	
610	0168921430000	$1,380.95	
611	0168921440000	$1,380.95	
612	0168921450000	$1,380.95	
613	0168921460000	$1,380.95	
614	0168921470000	$1,380.95	
615	0168921480000	$1,380.95	
616	0168921490000	$1,380.95	
617	0168921500000	$1,380.95	
618	0168921510000	$1,380.95	
619	0168921520000	$1,380.95	
620	0168921530000	$1,380.95	
621	0174711010000	$500.00	Annex No. 25
622	0174711020000	$500.00	
623	0174711030000	$500.00	
624	0174711040000	$500.00	
625	0174711050000	$500.00	
626	0174711060000	$500.00	
627	0174711070000	$500.00	
628	0174711080000	$500.00	
629	0174711090000	$500.00	
630	0174711100000	$500.00	
631	0174711110000	$500.00	
632	0174711120000	$500.00	
633	0174711130000	$500.00	
634	0174711140000	$500.00	
635	0174711150000	$500.00	
636	0174711160000	$500.00	
637	0174711170000	$500.00	
638	0174711180000	$500.00	
639	0174711190000	$500.00	
640	0174711200000	$500.00	
641	0174711210000	$500.00	
642	0174711220000	$500.00	
643	0174711230000	$500.00	
644	0174711240000	$500.00	
645	0174711250000	$500.00	
646	0174711260000	$500.00	
647	0174711270000	$500.00	
648	0174711280000	$500.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
649	0174711290000	$500.00	
650	0167462010000	$120.77	Annex No. 26
651	0167462020000	$120.77	
652	0167462030000	$120.77	
653	0167462040000	$120.77	
654	0167462050000	$120.77	
655	0167462060000	$120.77	
656	0167462070000	$120.77	
657	0167462080000	$120.77	
658	0167462090000	$120.77	
659	0167462100000	$120.77	
660	0167462110000	$120.77	
661	0167462120000	$120.77	
662	0167462130000	$120.77	
663	0167462140000	$120.77	
664	0167462150000	$120.77	
665	0167462160000	$120.77	
666	0167462170000	$120.77	
667	0167462180000	$120.77	
668	0167462190000	$120.77	
669	0167462200000	$120.77	
670	0167462210000	$120.77	
671	0167462220000	$120.77	
672	0167462230000	$120.77	
673	0167462240000	$120.77	
674	0167462250000	$120.77	
675	0167462260000	$120.77	
676	0167462270000	$120.77	
677	0167462280000	$120.77	
678	0167462290000	$120.77	
679	0167462300000	$120.77	
680	0167462310000	$120.77	
681	0167463010000	$120.77	
682	0167463020000	$120.77	
683	0167463030000	$120.77	
684	0167463040000	$120.77	
685	0167463050000	$120.77	
686	0167463060000	$120.77	
687	0167463070000	$120.77	
688	0167463080000	$120.77	
689	0167463090000	$120.77	
690	0167463100000	$120.77	
691	0167463110000	$120.77	
692	0167463120000	$120.77	
693	0167463130000	$120.77	
694	0167463140000	$120.77	
695	0167463150000	$120.77	
696	0167463160000	$120.77	
697	0167463170000	$120.77	
698	0167463180000	$120.77	
699	0167463190000	$120.77	
700	0167463200000	$120.77	
701	0167463210000	$120.77	
702	0167463220000	$120.77	
703	0167463230000	$120.77	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
704	0167463240000	$120.77
705	0167463250000	$120.77
706	0167463260000	$120.77
707	0167463270000	$120.77
708	0167463280000	$120.77
709	0167463290000	$120.77
710	0167463300000	$120.77
711	0167463310000	$120.77
712	0167463320000	$120.77
713	0167463330000	$120.77
714	0167463340000	$120.77
715	0167463350000	$120.77
716	0167463360000	$120.77
717	0167463370000	$120.77
718	0167463380000	$120.77
719	0167463390000	$120.77
720	0167463400000	$120.77
721	0167463410000	$120.77
722	0167463420000	$120.77
723	0167463430000	$120.77
724	0167463440000	$120.77
725	0167463450000	$120.77
726	0167463460000	$120.77
727	0167463470000	$120.77
728	0167463480000	$120.77
729	0167463490000	$120.77
730	0167463500000	$120.77
731	0167463510000	$120.77
732	0167463520000	$120.77
733	0167463530000	$120.77
734	0167463540000	$120.77
735	0167463550000	$120.77
736	0167463560000	$120.77
737	0167463570000	$120.77
738	0167463580000	$120.77
739	0167463590000	$120.77
740	0167463600000	$120.77
741	0167463610000	$120.77
742	0167463620000	$120.77
743	0167463630000	$120.77
744	0167463640000	$120.77
745	0167463650000	$120.77
746	0167463660000	$120.77
747	0167463670000	$120.77
748	0167463680000	$120.77
749	0167463690000	$120.77
750	0167473010000	$120.77
751	0167473020000	$120.77
752	0167473030000	$120.77
753	0167473040000	$120.77
754	0167473050000	$120.77
755	0167473060000	$120.77
756	0167473070000	$120.77
757	0167473080000	$120.77
758	0167473090000	$120.77

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
759	0167473100000	$120.77
760	0167473110000	$120.77
761	0167473120000	$120.77
762	0167473130000	$120.77
763	0167473140000	$120.77
764	0167473150000	$120.77
765	0167473160000	$120.77
766	0167473170000	$120.77
767	0167473180000	$120.77
768	0167473190000	$120.77
769	0167473200000	$120.77
770	0167473210000	$120.77
771	0167473220000	$120.77
772	0167473230000	$120.77
773	0167473240000	$120.77
774	0167473250000	$120.77
775	0167473260000	$120.77
776	0167473270000	$120.77
777	0167473280000	$120.77
778	0167473290000	$120.77
779	0167473300000	$120.77
780	0167473310000	$120.77
781	0167473320000	$120.77
782	0167473330000	$120.77
783	0167473340000	$120.77
784	0167473350000	$120.77
785	0167473360000	$120.77
786	0167473370000	$120.77
787	0167473380000	$120.77
788	0167473390000	$120.77
789	0167473400000	$120.77
790	0167473410000	$120.77
791	0167473420000	$120.77
792	0167473430000	$120.77
793	0167473440000	$120.77
794	0167473450000	$120.77
795	0167473460000	$120.77
796	0167473470000	$120.77
797	0167473480000	$120.77
798	0167473490000	$120.77
799	0167473500000	$120.77
800	0167473510000	$120.77
801	0167473520000	$120.77
802	0167473530000	$120.77
803	0167473540000	$120.77
804	0167473550000	$120.77
805	0167473560000	$120.77
806	0167473570000	$120.77
807	0167473580000	$120.77
808	0167473590000	$120.77
809	0167473600000	$120.77
810	0167473610000	$120.77
811	0167473620000	$120.77
812	0167473630000	$120.77
813	0167473640000	$120.77

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
814	0167473650000	$120.77	
815	0167473660000	$120.77	
816	0167473670000	$120.77	
817	0167473680000	$120.77	
818	0167473690000	$120.77	
819	0167474010000	$120.77	
820	0167474020000	$120.77	
821	0167474030000	$120.77	
822	0167474040000	$120.77	
823	0167474050000	$120.77	
824	0167474060000	$120.77	
825	0167474070000	$120.77	
826	0167474080000	$120.77	
827	0167474090000	$120.77	
828	0167474100000	$120.77	
829	0167474110000	$120.77	
830	0167474120000	$120.77	
831	0167474130000	$120.77	
832	0167474140000	$120.77	
833	0167474150000	$120.77	
834	0167474160000	$120.77	
835	0167474170000	$120.77	
836	0167474180000	$120.77	
837	0167474190000	$120.77	
838	0167474200000	$120.77	
839	0167474210000	$120.77	
840	0167474220000	$120.77	
841	0167474230000	$120.77	
842	0167474240000	$120.77	
843	0167474250000	$120.77	
844	0167474260000	$120.77	
845	0167474270000	$120.77	
846	0167474280000	$120.77	
847	0167474290000	$120.77	
848	0167474300000	$120.77	
849	0167474310000	$120.77	
850	0167474320000	$120.77	
851	0167474330000	$120.77	
852	0167474340000	$120.77	
853	0167474350000	$120.77	
854	0167474360000	$120.77	
855	0167474370000	$120.77	
856	0167474380000	$120.77	
857	0292032310000	$167.26	Annex No. 27
858	0292032360000	$3.32	
859	0292032480000	$4,829.57	
860	0167931010000	$410.09	Annex No. 29
861	0167931020000	$410.09	
862	0167931030000	$410.09	
863	0167931040000	$410.09	
864	0167931050000	$410.09	
865	0167931060000	$410.09	
866	0167931070000	$410.09	
867	0167931080000	$410.09	
868	0167931090000	$410.09	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
869	0167931100000	$410.09
870	0167931110000	$410.09
871	0167931120000	$410.09
872	0167931130000	$410.09
873	0167931140000	$410.09
874	0167931150000	$410.09
875	0167931160000	$410.09
876	0167931170000	$410.09
877	0167931180000	$410.09
878	0167931190000	$410.09
879	0167931200000	$410.09
880	0167931210000	$410.09
881	0167931220000	$410.09
882	0167931230000	$410.09
883	0167931240000	$410.09
884	0167931250000	$410.09
885	0167931260000	$410.09
886	0167931270000	$410.09
887	0167931280000	$410.09
888	0167931290000	$410.09
889	0167931300000	$410.09
890	0167931310000	$410.09
891	0167931320000	$410.09
892	0167931330000	$410.09
893	0167931340000	$410.09
894	0167931350000	$410.09
895	0167931360000	$410.09
896	0167931370000	$410.09
897	0167931380000	$410.09
898	0167931390000	$410.09
899	0167931400000	$410.09
900	0167931410000	$410.09
901	0167931420000	$410.09
902	0167931430000	$410.09
903	0167931440000	$410.09
904	0167931450000	$410.09
905	0167932010000	$410.09
906	0167932020000	$410.09
907	0167932030000	$410.09
908	0167932040000	$410.09
909	0167932050000	$410.09
910	0167932060000	$410.09
911	0167932070000	$410.09
912	0167932080000	$410.09
913	0167932090000	$410.09
914	0167932100000	$410.09
915	0167932110000	$410.09
916	0167932120000	$410.09
917	0167932130000	$410.09
918	0167932140000	$410.09
919	0167932150000	$410.09
920	0167932160000	$410.09
921	0167932170000	$410.09
922	0167932180000	$410.09
923	0167932190000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
924	0167932200000	$410.09
925	0167932210000	$410.09
926	0167932220000	$410.09
927	0167932230000	$410.09
928	0167932240000	$410.09
929	0167932250000	$410.09
930	0167932260000	$410.09
931	0167932270000	$410.09
932	0167932280000	$410.09
933	0167932290000	$410.09
934	0167932300000	$410.09
935	0167932310000	$410.09
936	0167932320000	$410.09
937	0167932330000	$410.09
938	0167932340000	$410.09
939	0167932350000	$410.09
940	0167932360000	$410.09
941	0167932370000	$410.09
942	0167932380000	$410.09
943	0167932390000	$410.09
944	0167932400000	$410.09
945	0167932410000	$410.09
946	0167932420000	$410.09
947	0167932430000	$410.09
948	0167932440000	$410.09
949	0167932450000	$410.09
950	0167932460000	$410.09
951	0167932470000	$410.09
952	0167932480000	$410.09
953	0167932490000	$410.09
954	0167932500000	$410.09
955	0167932510000	$410.09
956	0167932520000	$410.09
957	0167932530000	$410.09
958	0167932540000	$410.09
959	0167941010000	$410.09
960	0167941020000	$410.09
961	0167941030000	$410.09
962	0167941040000	$410.09
963	0167941050000	$410.09
964	0167941060000	$410.09
965	0167941070000	$410.09
966	0167941080000	$410.09
967	0167941090000	$410.09
968	0167941100000	$410.09
969	0167941110000	$410.09
970	0167941120000	$410.09
971	0167941130000	$410.09
972	0167941140000	$410.09
973	0167941150000	$410.09
974	0167941160000	$410.09
975	0167941170000	$410.09
976	0167941180000	$410.09
977	0167941190000	$410.09
978	0167941200000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
979	0167941210000	$410.09
980	0167941220000	$410.09
981	0167941230000	$410.09
982	0167941240000	$410.09
983	0167941250000	$410.09
984	0167941260000	$410.09
985	0167941270000	$410.09
986	0167941280000	$410.09
987	0167941290000	$410.09
988	0167941300000	$410.09
989	0167941310000	$410.09
990	0167941320000	$410.09
991	0167941330000	$410.09
992	0167941340000	$410.09
993	0167951010000	$410.09
994	0167951020000	$410.09
995	0167951030000	$410.09
996	0167951040000	$410.09
997	0167951050000	$410.09
998	0167951060000	$410.09
999	0167951070000	$410.09
1000	0167951080000	$410.09
1001	0167951090000	$410.09
1002	0167951100000	$410.09
1003	0167951110000	$410.09
1004	0167951120000	$410.09
1005	0167951130000	$410.09
1006	0167951140000	$410.09
1007	0167951150000	$410.09
1008	0167951160000	$410.09
1009	0167951170000	$410.09
1010	0167951180000	$410.09
1011	0167951190000	$410.09
1012	0167951200000	$410.09
1013	0167951210000	$410.09
1014	0167951220000	$410.09
1015	0167951230000	$410.09
1016	0167951240000	$410.09
1017	0167951250000	$410.09
1018	0167951260000	$410.09
1019	0167951270000	$410.09
1020	0167951280000	$410.09
1021	0167951290000	$410.09
1022	0167951300000	$410.09
1023	0167951310000	$410.09
1024	0167951320000	$410.09
1025	0167951330000	$410.09
1026	0167951340000	$410.09
1027	0167951350000	$410.09
1028	0167951360000	$410.09
1029	0167951370000	$410.09
1030	0167951380000	$410.09
1031	0167951390000	$410.09
1032	0167951400000	$410.09
1033	0167951410000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1034	0167951420000	$410.09
1035	0167951430000	$410.09
1036	0167951440000	$410.09
1037	0167951450000	$410.09
1038	0167951460000	$410.09
1039	0167951470000	$410.09
1040	0167951480000	$410.09
1041	0167951490000	$410.09
1042	0167951500000	$410.09
1043	0167951510000	$410.09
1044	0167951520000	$410.09
1045	0167951530000	$410.09
1046	0167951540000	$410.09
1047	0167951550000	$410.09
1048	0167951560000	$410.09
1049	0167951570000	$410.09
1050	0167951580000	$410.09
1051	0167951590000	$410.09
1052	0167951600000	$410.09
1053	0167951610000	$410.09
1054	0167951620000	$410.09
1055	0167951630000	$410.09
1056	0167961010000	$410.09
1057	0167961020000	$410.09
1058	0167961030000	$410.09
1059	0167961040000	$410.09
1060	0167961050000	$410.09
1061	0167961060000	$410.09
1062	0167961070000	$410.09
1063	0167961080000	$410.09
1064	0167961090000	$410.09
1065	0167961100000	$410.09
1066	0167961110000	$410.09
1067	0167961120000	$410.09
1068	0167961130000	$410.09
1069	0167961140000	$410.09
1070	0167961150000	$410.09
1071	0167961160000	$410.09
1072	0167961170000	$410.09
1073	0167961180000	$410.09
1074	0167961190000	$410.09
1075	0167961200000	$410.09
1076	0167961210000	$410.09
1077	0167961220000	$410.09
1078	0167961230000	$410.09
1079	0167961240000	$410.09
1080	0167961250000	$410.09
1081	0167961260000	$410.09
1082	0167961270000	$410.09
1083	0167961280000	$410.09
1084	0167961290000	$410.09
1085	0167961300000	$410.09
1086	0167961310000	$410.09
1087	0167961320000	$410.09
1088	0167961330000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1089	0167961340000	$410.09
1090	0167961350000	$410.09
1091	0167961360000	$410.09
1092	0167961370000	$410.09
1093	0167961380000	$410.09
1094	0167961390000	$410.09
1095	0167961400000	$410.09
1096	0167961410000	$410.09
1097	0167961420000	$410.09
1098	0167961430000	$410.09
1099	0167961440000	$410.09
1100	0167961450000	$410.09
1101	0167961460000	$410.09
1102	0167961470000	$410.09
1103	0167961480000	$410.09
1104	0167962010000	$410.09
1105	0167962020000	$410.09
1106	0167962030000	$410.09
1107	0167962040000	$410.09
1108	0167962050000	$410.09
1109	0167962060000	$410.09
1110	0167962070000	$410.09
1111	0167962080000	$410.09
1112	0167962090000	$410.09
1113	0167962100000	$410.09
1114	0167962110000	$410.09
1115	0167962120000	$410.09
1116	0167962130000	$410.09
1117	0167962140000	$410.09
1118	0167962150000	$410.09
1119	0167962160000	$410.09
1120	0167962170000	$410.09
1121	0167962180000	$410.09
1122	0167962190000	$410.09
1123	0167962200000	$410.09
1124	0167962210000	$410.09
1125	0167962220000	$410.09
1126	0167962230000	$410.09
1127	0167962240000	$410.09
1128	0167962250000	$410.09
1129	0167962260000	$410.09
1130	0167962270000	$410.09
1131	0167962280000	$410.09
1132	0167962290000	$410.09
1133	0167962300000	$410.09
1134	0167962310000	$410.09
1135	0167962320000	$410.09
1136	0167962330000	$410.09
1137	0167962340000	$410.09
1138	0167962350000	$410.09
1139	0167962360000	$410.09
1140	0167962370000	$410.09
1141	0167962380000	$410.09
1142	0167962390000	$410.09
1143	0167962400000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1144	0167962410000	$410.09
1145	0167962420000	$410.09
1146	0167962430000	$410.09
1147	0167962440000	$410.09
1148	0167962450000	$410.09
1149	0167962460000	$410.09
1150	0167962470000	$410.09
1151	0167962480000	$410.09
1152	0167962490000	$410.09
1153	0167962500000	$410.09
1154	0167962510000	$410.09
1155	0167962520000	$410.09
1156	0167962530000	$410.09
1157	0167962540000	$410.09
1158	0167962550000	$410.09
1159	0167962560000	$410.09
1160	0167962570000	$410.09
1161	0167962580000	$410.09
1162	0167962590000	$410.09
1163	0167962600000	$410.09
1164	0167962610000	$410.09
1165	0167962620000	$410.09
1166	0167962630000	$410.09
1167	0167962640000	$410.09
1168	0167962650000	$410.09
1169	0167962660000	$410.09
1170	0167962670000	$410.09
1171	0167962680000	$410.09
1172	0167962690000	$410.09
1173	0167962700000	$410.09
1174	0167962710000	$410.09
1175	0167962720000	$410.09
1176	0167962730000	$410.09
1176 Parcels	**Totals**	**$930,997.38**

EXHIBIT "B"
CITY OF REDLANDS
CFD 2004-1

District Landscaping	Maintenance Category	Tract/ Parcel Map No.	Landscape Areas	BUs	FY 26-27 Maximum Rates per Benefit Unit (1)	FY 26-27 Maximum Total Assessment	FY 26-27 Applied Rates per Benefit Unit	FY 26-27 Total Levy per Annexation (2)	FY 26-27 Percent of Max Tax
CFD 2004-1 Orig.	**K**	TR 16408	Please see Orig. ER	64.00	3.09% inc.			**$125,000.00**	**78.37%**
					$2,492.16	$159,498.37	$1,953.13		
Annexation 1	**B**	TR 16287	Drainage Basin	12.00	3.09% inc.			**$5,900.00**	**76.63%**
					$641.65	$7,699.77	$491.67		
Annexation 2	On Hold	TR 16586		n/a				**n/a**	**n/a**
					n/a	n/a	n/a		
Annexation 3	**A** (Construction has not started)	TTM 17253		37.00	3.09% inc.			**$0.00**	**0.00%**
					$427.35	$15,812.09	$0.00		
Annexation 4	**0**	PM 17353	Ford Street Median	5.80	3.09% inc.			**$13,200.00**	**82.30%**
					$2,765.23	$16,038.34	$2,275.86		
Annexation 5	**E**	CRA 826	California Street center Median	11.75	3.09% inc.			**$10,400.00**	**81.25%**
					$1,089.33	$12,799.67	$885.11		
Annexation 6	Failed	TR 14790-1		n/a				**n/a**	**n/a**
					n/a	n/a	n/a		
Annexation 7	On Hold	Parcel 2 of PM 15573		n/a				**n/a**	**n/a**
					n/a	n/a	n/a		
Annexation 8	**A** (Construction has not started)	TTM 16806		6.00	3.09% inc.			**$0.00**	**0.00%**
					$411.32	$2,467.94	$0.00		
Annexation 9	**A**	PM 18208	Redlands Median	42.55	3.09% inc.			**$14,100.00**	**86.35%**
					$383.76	$16,329.04	$331.37		
Annexation 10	On Hold	TR 18762		n/a				**n/a**	**n/a**
					n/a	n/a	n/a		
Annexation 11	**A** (BOA Maintained)	PM 19371	Street Trees on Lugonia & Wabash	39.90	3.09% inc.			**$0.00**	**0.00%**
					$368.86	$14,717.48	$0.00		
Annexation 12a	**G**	TR 16465	Street trees, parkways, basin, proposed Orange groves	61.00	3.09% inc.			**$64,200.00**	**87.90%**
					$1,197.40	$73,041.23	$1,052.46		
Annexation 12b	**H**	TR 16627	Street trees, parkways, basin, proposed Orange groves	20.00	3.09% inc.			**$23,700.00**	**88.55%**
					$1,338.27	$26,765.35	$1,185.00		
Annexation 12c	**G**	TR 18979, 19975 & 20079	Street trees, parkways, basin, proposed Orange groves	122.00	3.09% inc.			**$130,000.00**	**88.99%**
					$1,197.40	$146,082.45	$1,065.57		
Annexation 12d	**G**	TR 18979, 19975 & 20079	Street trees, parkways, basin, proposed Orange groves	14.00	3.09% inc.			**$15,000.00**	**89.48%**
					$1,197.40	$16,763.56	$1,071.43		
Annexation 13	**M** (HOA Maintained)	TR 18882	Street Trees	26.00	3.09% inc.			**$0.00**	**0.00%**
					$2,182.12	$56,735.05	$0.00		
Annexation 14	A	Planned Dev. # 1 PM 19496	California Median Owner to maintain Parkways	71.18	3.09% inc.			**$10,000.00**	**38.85%**
					$361.63	$25,740.59	$140.49		
Annexation 15	**A**	PM 18536-1	Ground cover, shrubs, turf, trees and palm trees	50.50	3.09% inc.			**$0.00**	**0.00%**
					$328.31	$16,579.49	$0.00		
Annexation 16	**I**	TR 18988	Riverview & Texas St.- Parks, slopes, parkways, median, open space, seating and monument structures	82.00	3.09% inc.			**$108,000.00**	**90.82%**
					$1,450.13	$118,911.07	$1,317.07		
Annexation 17	**H**	TR 17022	Ground cover, shrubs, citrus and palm trees	12.00	3.09% inc.			**$0.00**	**0.00%**
					$1,334.17	$16,010.02	$0.00		
Annexation 18	**E** (Owner Maintained)	PM 19465	Ground cover, shrubs, turf, trees and palm trees	17.80	3.09% inc.			**$0.00**	**0.00%**
					$897.70	$15,979.11	$0.00		
Annexation 19	**J**	TTM 19942	Sylvan Blvd & Wabash St.- Mulch, shrubs, trees, orange groves, trees and palm trees	34.00	3.09% inc.			**$46,000.00**	**89.59%**
					$1,510.21	$51,347.16	$1,352.94		
Annexation 20	**H**	TTM 19956	Highland Ave. & Wabash St.- Ground cover, shrubs, turf, trees and palm trees	40.00	3.09% inc.			**$46,000.00**	**90.10%**
					$1,276.30	$51,052.17	$1,150.00		
Annexation 21	**J**	TR 20126	Judson St & Lugonia Ave.- Ground cover, mulch, shrubs, orange groves, trees and basin	105.00	3.09% inc.			**$145,000.00**	**89.38%**
					$1,545.00	$162,224.99	$1,380.95		
Annexation 22	**A** (Owner Maintained)	PM 19981 CRA 900	Parkway	15.48	3.09% inc.			**$0.00**	**0.00%**
					$328.31	$5,082.19	$0.00		
Annexation 23	**B**	PM 18536	Parkway	9.55	3.09% inc.			**$0.00**	**0.00%**
					$443.81	$4,238.41	$0.00		
Annexation 24	**E**	CUP 1129	Parkway	3.95	3.09% inc.			**$0.00**	**0.00%**
					$824.22	$3,255.68	$0.00		
Annexation 25	**G**	TTM 20065	Moore St, Lot A, infiltration nasin, trenches, storm drain facilities, and street trees	29.00	3.09% inc.			**$14,500.00**	**53.38%**
					$936.67	$27,163.31	$500.00		

EXHIBIT "B"
CITY OF REDLANDS
CFD 2004-1

District Landscaping	Maintenance Category	Tract/ Parcel Map No.	Landscape Areas	BUs	FY 26-27 Maximum Rates per Benefit Unit [1]	FY 26-27 Maximum Total Assessment	FY 26-27 Applied Rates per Benefit Unit	FY 26-27 Total Levy per Annexation [2]	FY 26-27 Percent of Max Tax
Annexation 26	**B**	TR 20257	Texas & Pioneer - Parkway trees	207.00	3.09% inc. $403.31	$83,484.76	$120.77	**$25,000.00**	**29.95%**
Annexation 27	**A**	Mountain View Building Planned Dev. #4	Split Rail Fence & Concrete	45.14	3.09% inc. $288.08	$13,003.80	$110.77	**$5,000.00**	**38.45%**
Annexation 28	**C**	TR 20473	Parkway Trees	98.00	$450.00	$44,100.00	$0.00	**$0.00**	**0.00%**
Annexation 29	**D**	TR 20336	Parkways, Sports Park, and drainage basins	317.00	3.09% inc. $581.33	$184,281.13	$410.09	**$130,000.00**	**70.54%**
Annexation 30	**B**	TR 20528	Parkways, Contech Diversion Structureand biofileration system	117.00	$350.00	$40,950.00	$0.00	**$0.00**	**0.00%**
							Total	**$931,000.00**	

[1] The percentage increase listed is rounded to two decimal places, but has not been rounded when calculating the maximum rates for Fiscal Year 2026-27.

[2] Amount may be slightly off due to rounding.

Max/Applied Tax Rates per Benefit Unit for FY 26-27			
District	**Max Rates**	**Applied Rates**	**Notes**
Original District (TR 16408)	$2,492.16	$1,953.13	
Annexation No. 1 (TR 16287)	$641.65	$491.67	
Annexation No. 2 (TR 16586)	n/a	n/a	Annexation is on Hold
Annexation No. 3 (TTM 17253)	$427.35	$0.00	
Annexation No. 4 (PM 17353)	$2,765.23	$2,275.86	
Annexation No. 5 (CRA 826)	$1,089.33	$885.11	
Annexation No. 6 (TR 14790-1)	n/a	n/a	Annexation Failed
Annexation No. 7 (PM 15573)	n/a	n/a	Annexation is on Hold
Annexation No. 8 (TR 16806)	$411.32	$0.00	
Annexation No. 9 (PM 18208)	$383.76	$331.37	
Annexation No. 10 (TR 18762)	n/a	n/a	Annexation is on Hold
Annexation No. 11 (PM 19731)	$368.86	$0.00	Business Owner's Association maintained.
Annexation No. 12a (TR 16465)	$1,197.40	$1,052.46	
Annexation No. 12b (TR 16627)	$1,338.27	$1,185.00	
Annexation No. 12c (TR 18979, 19975 & 20079)	$1,197.40	$1,065.57	
Annexation No. 12d (TR 18979, 19975 & 20079)	$1,197.40	$1,071.43	
Annexation No. 13 (TR 18882)	$2,182.12	$0.00	HOA Maintained
Annexation No. 14 (PM 19496)	$361.63	$140.49	
Annexation No. 15 (PM 18536-1)	$328.31	$0.00	
Annexation No. 16 (TR 18988)	$1,450.13	$1,317.07	
Annexation No. 17 (TR 17022)	$1,334.17	$0.00	
Annexation No. 18 (PM 19465)	$897.70	$0.00	Owner Maintained
Annexation No. 19 (PM 19942)	$1,510.21	$1,352.94	
Annexation No. 20 (TM 19956)	$1,276.30	$1,150.00	
Annexation No. 21 (TR 20126)	$1,545.00	$1,380.95	
Annexation No. 22 (PM 19981 CRA 900)	$328.31	$0.00	Owner Maintained
Annexation No. 23 (PM 18536)	$443.81	$0.00	
Annexation No. 24 (CUP 1129)	$824.22	$0.00	
Annexation No. 25 (TTM 20065)	$936.67	$500.00	
Annexation No. 26 (TR20257)	$403.31	$120.77	
Annexation No. 27 (Planned Dev #4)	$288.08	$110.77	
Annexation No. 28 (TR 20473)	$450.00	$0.00	
Annexation No. 29 (TR 20036)	$581.33	$410.09	
Annexation No. 30 (TR 20528)	$350.00	$0.00	

RESOLUTION NO. 8809

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS LEVYING SPECIAL TAXES WITHIN CITY OF REDLANDS COMMUNITY FACILITIES DISTRICT NO. 2004-1 (TRACT MAP NO. 16408; TRACT MAP NO. 16287; TENTATIVE TRACT MAP NO. 17253; PARCEL MAP NO. 17353; COMMISSION REVIEW AND APPROVAL (CRA) NO. 826; TRACT MAP NO. 16806; PARCEL MAP NO. 18208; PARCEL MAP NO. 19371; TRACT MAP NO. 16465; TRACT MAP NO. 16627; TRACT MAP NO. 18979; TRACT MAP NO. 19975; TRACT MAP NO. 20079; TRACT MAP NO. 18882; PARCEL MAP NO. 19496; PARCEL MAP NO. 18536-1; TRACT MAP NO. 18988; TRACT MAP NO. 17022; PARCEL MAP NO. 19465; TRACT MAP NO. 19942; TRACT MAP NO. 19956; TRACT MAP NO. 20126; PARCEL MAP NO. 19981; PARCEL MAP NO. 18536; CONDITIONAL USE PERMIT (CUP) NO. 1129; TRACT MAP NO. 20065; TRACT MAP NO. 20257, PLANNED DEVELOPMENT NO. 4.. TRACT MAP NO. 20065, TRACT MAP NO. 20336, TRACT MAP NO. 20473, AND TRACT MAP NO. 20528.

WHEREAS, the City Council of the City of Redlands (the "City") has formed City of Redlands Community Facilities District No. 2004-1 (Tract Map No. 16408 – Centex Homes) and annexed Tract Map No. 16287 (Annexation No. 1), Tentative Tract Map No. 17253 (Annexation No. 3), Parcel Map No. 17353 (Annexation No. 4), CRA No. 826 (Annexation No. 5), Tract Map No. 16806 (Annexation No. 8), Parcel Map No. 18208 (Annexation No. 9), Parcel Map No. 19371 (Annexation No. 11), Tract Map No. 16465, Tract Map No. 16627, Tract Map No. 18979, Tract Map No. 19975 and Tract Map No. 20079 (Annexation No. 12), Tract Map No. 18882 (Annexation No. 13), Parcel Map No. 19496 (Annexation No. 14), Parcel Map No. 18536-1 (Annexation No. 15), Tract Map No. 18988 (Annexation No. 16), Tract Map No. 17022 (Annexation No. 17), Parcel Map No. 19465 (Annexation No. 18), Tract Map No. 19942 (Annexation No. 19), Tract Map No. 19956 (Annexation No. 20), Tract Map No. 20126 (Annexation No. 21), Parcel Map No. 19981 (Annexation No. 22), Parcel Map No. 18536 (Annexation No. 23), CUP No. 1129 (Annexation No. 24), Tract Map No. 20065 (Annexation No. 25), Tract Map No. 20257 (Annexation No. 26), Planned Development No. 4 (Annexation No. 27), and Tract Map No. 20473 (Annexation No. 28), and Tract Map No. 20336 (Annexation No. 29), and Tract Map No.20528 (Annexation No. 30) into the City of Redlands Community Facilities District No. 2004-1 (the "Community Facilities District"), under and pursuant to the Mello-Roos Community Facilities Act of 1982 (the "Act"); and

WHEREAS, the City Council, as the legislative body of the Community Facilities District, is authorized under the Act to levy special taxes (the "Special Taxes") to pay for the costs of certain facilities and to authorize the issuance of bonds secured by the Special Taxes under the Act; and

WHEREAS, the City Council, pursuant to Ordinance No. 2584, adopted by the City Council of the City on August 3, 2004, and Resolution No. 6481, adopted on May 2, 2006, authorized and levied the Special Taxes within the Community Facilities District; and

WHEREAS, Section 53340 of the Act provides that the legislative body of a community facilities district may provide, by resolution, for the levy of the special tax in the current year or future tax years at the same rate or at a lower rate than the rate provided by ordinance, if the resolution is adopted and a certified list of all parcels subject to the special tax levy including the amount of the tax to be levied on each parcel for the applicable tax year, is filed by the clerk or

other official designated by the legislative body with the county auditor on or before the 10th day of August of that tax year; and

WHEREAS, the City Council desires to levy the Special Taxes within the Community Facilities District for Fiscal Year 2026-2027;

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Redlands as follows:

Section 1. All of the above recitals are true and correct.

Section 2. The City Council hereby levies the Special Taxes for the Fiscal Year 2026-2027 at the applied rates, up to the maximum, and with respect to the parcels as set forth in Exhibit A and Exhibit B hereto; provided, however, that the City Manager or the Finance Director of the City is hereby authorized, prior to the submission to the San Bernardino County Auditor/Controller and upon consultation with the City's special tax consultant, Webb Municipal Finance, LLC (a) to make any necessary modifications to such Special Taxes to correct any errors, omissions or inconsistencies in the listing or categorization of parcels to be taxed (provided that any such modifications shall not result in an increase in the Special Tax applicable to any category of parcels), or (b) to lower such Special Tax rates to the extent such officer deems necessary upon receipt of the final pricing information. The City Clerk of the City is hereby authorized and directed to file with the San Bernardino County Auditor/Controller no later than August 10, 2026, a certified list of all parcels subject to the Special Tax levy including the amount of the Special Tax to be levied on each parcel for Fiscal Year 2026-2027.

Section 3. The officers and agents of the City are, and each of them hereby is, authorized and directed to execute and deliver any and all documents and instruments and to do and cause to be done any and all acts and things necessary or proper for carrying out the levy of the Special Taxes for Fiscal Year 2026-2027 as provided in this Resolution.

Section 4. All actions heretofore taken by the officers and agents of the City with respect to the levy of the Special Taxes for Fiscal Year 2026-2027 are hereby approved, confirmed and ratified.

Section 5. This Resolution shall take effect immediately upon its adoption.

APPROVED and ADOPTED by the City Council of the City of Redlands on July 7, 2026.

Mario Saucedo, Mayor

ATTEST:

Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, hereby certify that the foregoing Resolution was duly adopted at a regular meeting thereof, held on the 7th day of July, 2026, by the following vote:

AYES: Councilmembers Barich, Tejeda, Davis, Shaw; Mayor Saucedo
NOES: None
ABSENT: None
ABSTAIN: None

Jeanne Donaldson, City Clerk

Exhibit A – Annexation Levy Summary by Assessor's Parcel Number

Exhibit B – Annexation Listing with Maximum and Applied Rates

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
1	0174651010000	$1,953.13	Original
2	0174651020000	$1,953.13	
3	0174651030000	$1,953.13	
4	0174651040000	$1,953.13	
5	0174651050000	$1,953.13	
6	0174651060000	$1,953.13	
7	0174651070000	$1,953.13	
8	0174651080000	$1,953.13	
9	0174651090000	$1,953.13	
10	0174651100000	$1,953.13	
11	0174651110000	$1,953.13	
12	0174651120000	$1,953.13	
13	0174651130000	$1,953.13	
14	0174651140000	$1,953.13	
15	0174651150000	$1,953.13	
16	0174651160000	$1,953.13	
17	0174651170000	$1,953.13	
18	0174651180000	$1,953.13	
19	0174651190000	$1,953.13	
20	0174651200000	$1,953.13	
21	0174651210000	$1,953.13	
22	0174651220000	$1,953.13	
23	0174651230000	$1,953.13	
24	0174651240000	$1,953.13	
25	0174651250000	$1,953.13	
26	0174651260000	$1,953.13	
27	0174651270000	$1,953.13	
28	0174651280000	$1,953.13	
29	0174651290000	$1,953.13	
30	0174651300000	$1,953.13	
31	0174651310000	$1,953.13	
32	0174651320000	$1,953.13	
33	0174651330000	$1,953.13	
34	0174651340000	$1,953.13	
35	0174661010000	$1,953.13	
36	0174661020000	$1,953.13	
37	0174661030000	$1,953.13	
38	0174661040000	$1,953.13	
39	0174661050000	$1,953.13	
40	0174661060000	$1,953.13	
41	0174661070000	$1,953.13	
42	0174661080000	$1,953.13	
43	0174661090000	$1,953.13	
44	0174661100000	$1,953.13	
45	0174661110000	$1,953.13	
46	0174661120000	$1,953.13	
47	0174661130000	$1,953.13	
48	0174661140000	$1,953.13	
49	0174661150000	$1,953.13	
50	0174661160000	$1,953.13	
51	0174661170000	$1,953.13	
52	0174661180000	$1,953.13	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
53	0174661190000	$1,953.13	
54	0174661200000	$1,953.13	
55	0174661210000	$1,953.13	
56	0174661220000	$1,953.13	
57	0174661230000	$1,953.13	
58	0174661240000	$1,953.13	
59	0174661250000	$1,953.13	
60	0174661260000	$1,953.13	
61	0174661270000	$1,953.13	
62	0174661280000	$1,953.13	
63	0174661290000	$1,953.13	
64	0174661300000	$1,953.13	
65	1212371080000	$491.67	Annex No. 1
66	1212371090000	$491.67	
67	1212371100000	$491.67	
68	1212371110000	$491.67	
69	1212371120000	$491.67	
70	1212371130000	$491.67	
71	1212371140000	$491.67	
72	1212371150000	$491.67	
73	1212371160000	$491.67	
74	1212371170000	$491.67	
75	1212371180000	$491.67	
76	1212371190000	$491.67	
77	0174252200000	$4,324.13	Annex No. 4
78	0174691060000	$261.72	
79	0174691070000	$261.72	
80	0174691080000	$261.72	
81	0174691090000	$261.72	
82	0174691100000	$261.72	
83	0174691110000	$261.72	
84	0174691120000	$261.72	
85	0174691130000	$261.72	
86	0174691140000	$261.72	
87	0174691150000	$261.72	
88	0174691160000	$357.64	
89	0174691170000	$357.64	
90	0174691180000	$357.64	
91	0174691190000	$357.64	
92	0174691200000	$357.64	
93	0174691210000	$357.64	
94	0174691220000	$357.64	
95	0174691230000	$261.72	
96	0174691240000	$261.72	
97	0174691250000	$261.72	
98	0174691260000	$261.72	
99	0174691270000	$261.72	
100	0174691280000	$261.72	
101	0174691290000	$261.72	
102	0174691300000	$261.72	
103	0174691310000	$261.72	
104	0174691320000	$261.72	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
105	0174691330000	$284.49	
106	0174691340000	$284.49	
107	0174691350000	$284.49	
108	0174691360000	$284.49	
109	0292061490000	$7,080.84	Annex No. 5
110	0292061500000	$3,319.15	
111	0292631020000	$454.83	Annex No. 9
112	0292631030000	$454.83	
113	0292631040000	$454.83	
114	0292631050000	$454.83	
115	0292631060000	$454.83	
116	0292631070000	$454.83	
117	0292631080000	$454.83	
118	0292631090000	$454.83	
119	0292631100000	$454.83	
120	0292631110000	$454.83	
121	0292631120000	$454.83	
122	0292631130000	$454.83	
123	0292631140000	$454.83	
124	0292631150000	$454.83	
125	0292631160000	$454.83	
126	0292631170000	$454.83	
127	0292631180000	$454.83	
128	0292631190000	$454.83	
129	0292631200000	$454.83	
130	0292631210000	$454.83	
131	0292631220000	$454.83	
132	0292631230000	$454.83	
133	0292631240000	$454.83	
134	0292631250000	$454.83	
135	0292631260000	$454.83	
136	0292631270000	$454.83	
137	0292631280000	$454.83	
138	0292631290000	$454.83	
139	0292631300000	$454.83	
140	0292631310000	$454.83	
141	0292631320000	$454.83	
142	1212451010000	$1,052.46	Annex No. 12a
143	1212451020000	$1,052.46	
144	1212451030000	$1,052.46	
145	1212451040000	$1,052.46	
146	1212451050000	$1,052.46	
147	1212451060000	$1,052.46	
148	1212451070000	$1,052.46	
149	1212451080000	$1,052.46	
150	1212451090000	$1,052.46	
151	1212451100000	$1,052.46	
152	1212451110000	$1,052.46	
153	1212451120000	$1,052.46	
154	1212451130000	$1,052.46	
155	1212451140000	$1,052.46	
156	1212451150000	$1,052.46	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
157	1212451160000	$1,052.46	
158	1212451170000	$1,052.46	
159	1212451180000	$1,052.46	
160	1212451190000	$1,052.46	
161	1212451200000	$1,052.46	
162	1212451210000	$1,052.46	
163	1212451220000	$1,052.46	
164	1212451230000	$1,052.46	
165	1212451240000	$1,052.46	
166	1212451250000	$1,052.46	
167	1212451260000	$1,052.46	
168	1212451270000	$1,052.46	
169	1212451280000	$1,052.46	
170	1212451290000	$1,052.46	
171	1212451300000	$1,052.46	
172	1212451310000	$1,052.46	
173	1212451320000	$1,052.46	
174	1212451330000	$1,052.46	
175	1212451340000	$1,052.46	
176	1212451350000	$1,052.46	
177	1212451360000	$1,052.46	
178	1212451370000	$1,052.46	
179	1212451380000	$1,052.46	
180	1212451390000	$1,052.46	
181	1212451400000	$1,052.46	
182	1212451410000	$1,052.46	
183	1212451420000	$1,052.46	
184	1212451430000	$1,052.46	
185	1212451440000	$1,052.46	
186	1212451450000	$1,052.46	
187	1212451460000	$1,052.46	
188	1212451470000	$1,052.46	
189	1212451480000	$1,052.46	
190	1212451490000	$1,052.46	
191	1212451500000	$1,052.46	
192	1212451510000	$1,052.46	
193	1212451520000	$1,052.46	
194	1212451530000	$1,052.46	
195	1212451540000	$1,052.46	
196	1212451550000	$1,052.46	
197	1212451560000	$1,052.46	
198	1212451570000	$1,052.46	
199	1212451580000	$1,052.46	
200	1212451590000	$1,052.46	
201	1212451600000	$1,052.46	
202	1212451610000	$1,052.46	
203	0168891010000	$1,185.00	Annex. No. 12b
204	0168891020000	$1,185.00	
205	0168891030000	$1,185.00	
206	0168891040000	$1,185.00	
207	0168891050000	$1,185.00	
208	0168891060000	$1,185.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
209	0168891070000	$1,185.00	
210	0168891080000	$1,185.00	
211	0168891090000	$1,185.00	
212	0168891100000	$1,185.00	
213	0168891110000	$1,185.00	
214	0168891120000	$1,185.00	
215	0168891130000	$1,185.00	
216	0168891140000	$1,185.00	
217	0168891150000	$1,185.00	
218	0168891160000	$1,185.00	
219	0168891170000	$1,185.00	
220	0168891180000	$1,185.00	
221	0168891190000	$1,185.00	
222	0168891200000	$1,185.00	
223	0168071170000	$1,065.57	Annex. No. 12c
224	0168071180000	$1,065.57	
225	0168071190000	$1,065.57	
226	0168071200000	$1,065.57	
227	0168071210000	$1,065.57	
228	0168071220000	$1,065.57	
229	0168071230000	$1,065.57	
230	0168071240000	$1,065.57	
231	0168071250000	$1,065.57	
232	0168071260000	$1,065.57	
233	0168071270000	$1,065.57	
234	0168071280000	$1,065.57	
235	0168071290000	$1,065.57	
236	0168071300000	$1,065.57	
237	0168071310000	$1,065.57	
238	0168071320000	$1,065.57	
239	0168071330000	$1,065.57	
240	0168071340000	$1,065.57	
241	0168071350000	$1,065.57	
242	0168071360000	$1,065.57	
243	0168071370000	$1,065.57	
244	0168071380000	$1,065.57	
245	0168071390000	$1,065.57	
246	0168071400000	$1,065.57	
247	0168071410000	$1,065.57	
248	0168071420000	$1,065.57	
249	0168071430000	$1,065.57	
250	0168071440000	$1,065.57	
251	0168071450000	$1,065.57	
252	0168071460000	$1,065.57	
253	0168071470000	$1,065.57	
254	0168071480000	$1,065.57	
255	0168071490000	$1,065.57	
256	0168071500000	$1,065.57	
257	0168071510000	$1,065.57	
258	0168071520000	$1,065.57	
259	0168071530000	$1,065.57	
260	0168071540000	$1,065.57	
261	0168071550000	$1,065.57	
262	0168071560000	$1,065.57	
263	0168071570000	$1,065.57	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
264	0168071580000	$1,065.57
265	0168071590000	$1,065.57
266	0168071600000	$1,065.57
267	0168071610000	$1,065.57
268	0168071620000	$1,065.57
269	0168071630000	$1,065.57
270	0168071640000	$1,065.57
271	0168071650000	$1,065.57
272	0168071660000	$1,065.57
273	0168071670000	$1,065.57
274	0168071680000	$1,065.57
275	0168071690000	$1,065.57
276	0168071700000	$1,065.57
277	0168071710000	$1,065.57
278	0168901010000	$1,065.57
279	0168901020000	$1,065.57
280	0168901030000	$1,065.57
281	0168901040000	$1,065.57
282	0168901050000	$1,065.57
283	0168901060000	$1,065.57
284	0168901070000	$1,065.57
285	0168901080000	$1,065.57
286	0168901090000	$1,065.57
287	0168901100000	$1,065.57
288	0168901110000	$1,065.57
289	0168901120000	$1,065.57
290	0168901130000	$1,065.57
291	0168901140000	$1,065.57
292	0168901150000	$1,065.57
293	0168901160000	$1,065.57
294	0168901170000	$1,065.57
295	0168901180000	$1,065.57
296	0168901190000	$1,065.57
297	0168901200000	$1,065.57
298	0168901210000	$1,065.57
299	0168901220000	$1,065.57
300	0168901230000	$1,065.57
301	0168901240000	$1,065.57
302	0168901250000	$1,065.57
303	0168901260000	$1,065.57
304	0168901270000	$1,065.57
305	0168901280000	$1,065.57
306	0168901290000	$1,065.57
307	0168901300000	$1,065.57
308	0168901310000	$1,065.57
309	0168901320000	$1,065.57
310	0168901330000	$1,065.57
311	0168901340000	$1,065.57
312	0168901350000	$1,065.57
313	0168901360000	$1,065.57
314	0168901370000	$1,065.57
315	0168901380000	$1,065.57
316	0168901390000	$1,065.57
317	0168901400000	$1,065.57
318	0168901410000	$1,065.57

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
319	0168901420000	$1,065.57	
320	0168901430000	$1,065.57	
321	0168901440000	$1,065.57	
322	0168901450000	$1,065.57	
323	0168901460000	$1,065.57	
324	0168901470000	$1,065.57	
325	0168901480000	$1,065.57	
326	0168901490000	$1,065.57	
327	0168901500000	$1,065.57	
328	0168901510000	$1,065.57	
329	0168901520000	$1,065.57	
330	0168901530000	$1,065.57	
331	0168901540000	$1,065.57	
332	0168901550000	$1,065.57	
333	0168901560000	$1,065.57	
334	0168901570000	$1,065.57	
335	0168901580000	$1,065.57	
336	0168901590000	$1,065.57	
337	0168901600000	$1,065.57	
338	0168901610000	$1,065.57	
339	0168901620000	$1,065.57	
340	0168901630000	$1,065.57	
341	0168901640000	$1,065.57	
342	0168901650000	$1,065.57	
343	0168901660000	$1,065.57	
344	0168901670000	$1,065.57	
345	0168071760000	$1,071.43	Annex No. 12d
346	0168071770000	$1,071.43	
347	0168071780000	$1,071.43	
348	0168071790000	$1,071.43	
349	0168071800000	$1,071.43	
350	0168071810000	$1,071.43	
351	0168071820000	$1,071.43	
352	0168071830000	$1,071.43	
353	0168071840000	$1,071.43	
354	0168071850000	$1,071.43	
355	0168071860000	$1,071.43	
356	0168071870000	$1,071.43	
357	0168071880000	$1,071.43	
358	0168071890000	$1,071.43	
359	0292053160000	$10,000.08	Annex No. 14
360	0167422010000	$1,317.07	Annex No. 16
361	0167422020000	$1,317.07	
362	0167422030000	$1,317.07	
363	0167422040000	$1,317.07	
364	0167422050000	$1,317.07	
365	0167422060000	$1,317.07	
366	0167422070000	$1,317.07	
367	0167422080000	$1,317.07	
368	0167422090000	$1,317.07	
369	0167422100000	$1,317.07	
370	0167422110000	$1,317.07	
371	0167422120000	$1,317.07	
372	0167422130000	$1,317.07	
373	0167422140000	$1,317.07	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
374	0167422150000	$1,317.07
375	0167422160000	$1,317.07
376	0167422170000	$1,317.07
377	0167422180000	$1,317.07
378	0167422190000	$1,317.07
379	0167422200000	$1,317.07
380	0167422210000	$1,317.07
381	0167422220000	$1,317.07
382	0167422230000	$1,317.07
383	0167422240000	$1,317.07
384	0167422250000	$1,317.07
385	0167422260000	$1,317.07
386	0167422270000	$1,317.07
387	0167422280000	$1,317.07
388	0167422290000	$1,317.07
389	0167422300000	$1,317.07
390	0167422310000	$1,317.07
391	0167422320000	$1,317.07
392	0167422330000	$1,317.07
393	0167422340000	$1,317.07
394	0167422350000	$1,317.07
395	0167422360000	$1,317.07
396	0167422370000	$1,317.07
397	0167422380000	$1,317.07
398	0167422390000	$1,317.07
399	0167422400000	$1,317.07
400	0167422410000	$1,317.07
401	0167422420000	$1,317.07
402	0167432010000	$1,317.07
403	0167432020000	$1,317.07
404	0167432030000	$1,317.07
405	0167432040000	$1,317.07
406	0167432050000	$1,317.07
407	0167432060000	$1,317.07
408	0167432070000	$1,317.07
409	0167432080000	$1,317.07
410	0167432090000	$1,317.07
411	0167432100000	$1,317.07
412	0167432110000	$1,317.07
413	0167432120000	$1,317.07
414	0167432130000	$1,317.07
415	0167432140000	$1,317.07
416	0167432150000	$1,317.07
417	0167432160000	$1,317.07
418	0167432170000	$1,317.07
419	0167432180000	$1,317.07
420	0167432190000	$1,317.07
421	0167432200000	$1,317.07
422	0167432210000	$1,317.07
423	0167432220000	$1,317.07
424	0167432230000	$1,317.07
425	0167432240000	$1,317.07
426	0167432250000	$1,317.07
427	0167432260000	$1,317.07
428	0167432270000	$1,317.07

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
429	0167432280000	$1,317.07	
430	0167432290000	$1,317.07	
431	0167432300000	$1,317.07	
432	0167432310000	$1,317.07	
433	0167432320000	$1,317.07	
434	0167432330000	$1,317.07	
435	0167432340000	$1,317.07	
436	0167432350000	$1,317.07	
437	0167432360000	$1,317.07	
438	0167432370000	$1,317.07	
439	0167432380000	$1,317.07	
440	0167432390000	$1,317.07	
441	0167432400000	$1,317.07	
442	0299431010000	$1,352.94	Annex No. 19
443	0299431020000	$1,352.94	
444	0299431030000	$1,352.94	
445	0299431040000	$1,352.94	
446	0299431050000	$1,352.94	
447	0299431060000	$1,352.94	
448	0299431070000	$1,352.94	
449	0299431080000	$1,352.94	
450	0299431090000	$1,352.94	
451	0299431100000	$1,352.94	
452	0299431110000	$1,352.94	
453	0299431120000	$1,352.94	
454	0299431130000	$1,352.94	
455	0299431140000	$1,352.94	
456	0299431150000	$1,352.94	
457	0299431160000	$1,352.94	
458	0299431170000	$1,352.94	
459	0299431180000	$1,352.94	
460	0299431190000	$1,352.94	
461	0299431200000	$1,352.94	
462	0299431210000	$1,352.94	
463	0299431220000	$1,352.94	
464	0299431230000	$1,352.94	
465	0299431240000	$1,352.94	
466	0299431250000	$1,352.94	
467	0299431260000	$1,352.94	
468	0299431270000	$1,352.94	
469	0299431280000	$1,352.94	
470	0299431290000	$1,352.94	
471	0299431300000	$1,352.94	
472	0299431310000	$1,352.94	
473	0299431320000	$1,352.94	
474	0299431330000	$1,352.94	
475	0299431340000	$1,352.94	
476	0299421010000	$1,150.00	Annex No. 20
477	0299421020000	$1,150.00	
478	0299421030000	$1,150.00	
479	0299421040000	$1,150.00	
480	0299421050000	$1,150.00	
481	0299421060000	$1,150.00	
482	0299421070000	$1,150.00	
483	0299421080000	$1,150.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
484	0299421090000	$1,150.00	
485	0299421100000	$1,150.00	
486	0299421110000	$1,150.00	
487	0299421120000	$1,150.00	
488	0299421130000	$1,150.00	
489	0299421140000	$1,150.00	
490	0299421150000	$1,150.00	
491	0299421160000	$1,150.00	
492	0299421170000	$1,150.00	
493	0299421180000	$1,150.00	
494	0299421190000	$1,150.00	
495	0299421200000	$1,150.00	
496	0299421210000	$1,150.00	
497	0299421220000	$1,150.00	
498	0299421230000	$1,150.00	
499	0299421240000	$1,150.00	
500	0299421250000	$1,150.00	
501	0299421260000	$1,150.00	
502	0299421270000	$1,150.00	
503	0299421280000	$1,150.00	
504	0299421290000	$1,150.00	
505	0299421300000	$1,150.00	
506	0299421310000	$1,150.00	
507	0299421320000	$1,150.00	
508	0299421330000	$1,150.00	
509	0299421340000	$1,150.00	
510	0299421350000	$1,150.00	
511	0299421360000	$1,150.00	
512	0299421370000	$1,150.00	
513	0299421380000	$1,150.00	
514	0299421390000	$1,150.00	
515	0299421400000	$1,150.00	
516	0168911010000	$1,380.95	Annex No. 21
517	0168911020000	$1,380.95	
518	0168911030000	$1,380.95	
519	0168911040000	$1,380.95	
520	0168911050000	$1,380.95	
521	0168911060000	$1,380.95	
522	0168911070000	$1,380.95	
523	0168911080000	$1,380.95	
524	0168911090000	$1,380.95	
525	0168911100000	$1,380.95	
526	0168911110000	$1,380.95	
527	0168911120000	$1,380.95	
528	0168911130000	$1,380.95	
529	0168911140000	$1,380.95	
530	0168911150000	$1,380.95	
531	0168911160000	$1,380.95	
532	0168911170000	$1,380.95	
533	0168911180000	$1,380.95	
534	0168911190000	$1,380.95	
535	0168911200000	$1,380.95	
536	0168911210000	$1,380.95	
537	0168911220000	$1,380.95	
538	0168911230000	$1,380.95	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
539	0168911240000	$1,380.95
540	0168911250000	$1,380.95
541	0168911260000	$1,380.95
542	0168911270000	$1,380.95
543	0168911280000	$1,380.95
544	0168911290000	$1,380.95
545	0168911300000	$1,380.95
546	0168911310000	$1,380.95
547	0168911320000	$1,380.95
548	0168911330000	$1,380.95
549	0168911340000	$1,380.95
550	0168911350000	$1,380.95
551	0168911360000	$1,380.95
552	0168911370000	$1,380.95
553	0168911380000	$1,380.95
554	0168911390000	$1,380.95
555	0168911400000	$1,380.95
556	0168911410000	$1,380.95
557	0168911420000	$1,380.95
558	0168911430000	$1,380.95
559	0168911440000	$1,380.95
560	0168911450000	$1,380.95
561	0168911460000	$1,380.95
562	0168911470000	$1,380.95
563	0168911480000	$1,380.95
564	0168911490000	$1,380.95
565	0168911500000	$1,380.95
566	0168911510000	$1,380.95
567	0168911520000	$1,380.95
568	0168921010000	$1,380.95
569	0168921020000	$1,380.95
570	0168921030000	$1,380.95
571	0168921040000	$1,380.95
572	0168921050000	$1,380.95
573	0168921060000	$1,380.95
574	0168921070000	$1,380.95
575	0168921080000	$1,380.95
576	0168921090000	$1,380.95
577	0168921100000	$1,380.95
578	0168921110000	$1,380.95
579	0168921120000	$1,380.95
580	0168921130000	$1,380.95
581	0168921140000	$1,380.95
582	0168921150000	$1,380.95
583	0168921160000	$1,380.95
584	0168921170000	$1,380.95
585	0168921180000	$1,380.95
586	0168921190000	$1,380.95
587	0168921200000	$1,380.95
588	0168921210000	$1,380.95
589	0168921220000	$1,380.95
590	0168921230000	$1,380.95
591	0168921240000	$1,380.95
592	0168921250000	$1,380.95
593	0168921260000	$1,380.95

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
594	0168921270000	$1,380.95	
595	0168921280000	$1,380.95	
596	0168921290000	$1,380.95	
597	0168921300000	$1,380.95	
598	0168921310000	$1,380.95	
599	0168921320000	$1,380.95	
600	0168921330000	$1,380.95	
601	0168921340000	$1,380.95	
602	0168921350000	$1,380.95	
603	0168921360000	$1,380.95	
604	0168921370000	$1,380.95	
605	0168921380000	$1,380.95	
606	0168921390000	$1,380.95	
607	0168921400000	$1,380.95	
608	0168921410000	$1,380.95	
609	0168921420000	$1,380.95	
610	0168921430000	$1,380.95	
611	0168921440000	$1,380.95	
612	0168921450000	$1,380.95	
613	0168921460000	$1,380.95	
614	0168921470000	$1,380.95	
615	0168921480000	$1,380.95	
616	0168921490000	$1,380.95	
617	0168921500000	$1,380.95	
618	0168921510000	$1,380.95	
619	0168921520000	$1,380.95	
620	0168921530000	$1,380.95	
621	0174711010000	$500.00	Annex No. 25
622	0174711020000	$500.00	
623	0174711030000	$500.00	
624	0174711040000	$500.00	
625	0174711050000	$500.00	
626	0174711060000	$500.00	
627	0174711070000	$500.00	
628	0174711080000	$500.00	
629	0174711090000	$500.00	
630	0174711100000	$500.00	
631	0174711110000	$500.00	
632	0174711120000	$500.00	
633	0174711130000	$500.00	
634	0174711140000	$500.00	
635	0174711150000	$500.00	
636	0174711160000	$500.00	
637	0174711170000	$500.00	
638	0174711180000	$500.00	
639	0174711190000	$500.00	
640	0174711200000	$500.00	
641	0174711210000	$500.00	
642	0174711220000	$500.00	
643	0174711230000	$500.00	
644	0174711240000	$500.00	
645	0174711250000	$500.00	
646	0174711260000	$500.00	
647	0174711270000	$500.00	
648	0174711280000	$500.00	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
649	0174711290000	$500.00	
650	0167462010000	$120.77	Annex No. 26
651	0167462020000	$120.77	
652	0167462030000	$120.77	
653	0167462040000	$120.77	
654	0167462050000	$120.77	
655	0167462060000	$120.77	
656	0167462070000	$120.77	
657	0167462080000	$120.77	
658	0167462090000	$120.77	
659	0167462100000	$120.77	
660	0167462110000	$120.77	
661	0167462120000	$120.77	
662	0167462130000	$120.77	
663	0167462140000	$120.77	
664	0167462150000	$120.77	
665	0167462160000	$120.77	
666	0167462170000	$120.77	
667	0167462180000	$120.77	
668	0167462190000	$120.77	
669	0167462200000	$120.77	
670	0167462210000	$120.77	
671	0167462220000	$120.77	
672	0167462230000	$120.77	
673	0167462240000	$120.77	
674	0167462250000	$120.77	
675	0167462260000	$120.77	
676	0167462270000	$120.77	
677	0167462280000	$120.77	
678	0167462290000	$120.77	
679	0167462300000	$120.77	
680	0167462310000	$120.77	
681	0167463010000	$120.77	
682	0167463020000	$120.77	
683	0167463030000	$120.77	
684	0167463040000	$120.77	
685	0167463050000	$120.77	
686	0167463060000	$120.77	
687	0167463070000	$120.77	
688	0167463080000	$120.77	
689	0167463090000	$120.77	
690	0167463100000	$120.77	
691	0167463110000	$120.77	
692	0167463120000	$120.77	
693	0167463130000	$120.77	
694	0167463140000	$120.77	
695	0167463150000	$120.77	
696	0167463160000	$120.77	
697	0167463170000	$120.77	
698	0167463180000	$120.77	
699	0167463190000	$120.77	
700	0167463200000	$120.77	
701	0167463210000	$120.77	
702	0167463220000	$120.77	
703	0167463230000	$120.77	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
704	0167463240000	$120.77
705	0167463250000	$120.77
706	0167463260000	$120.77
707	0167463270000	$120.77
708	0167463280000	$120.77
709	0167463290000	$120.77
710	0167463300000	$120.77
711	0167463310000	$120.77
712	0167463320000	$120.77
713	0167463330000	$120.77
714	0167463340000	$120.77
715	0167463350000	$120.77
716	0167463360000	$120.77
717	0167463370000	$120.77
718	0167463380000	$120.77
719	0167463390000	$120.77
720	0167463400000	$120.77
721	0167463410000	$120.77
722	0167463420000	$120.77
723	0167463430000	$120.77
724	0167463440000	$120.77
725	0167463450000	$120.77
726	0167463460000	$120.77
727	0167463470000	$120.77
728	0167463480000	$120.77
729	0167463490000	$120.77
730	0167463500000	$120.77
731	0167463510000	$120.77
732	0167463520000	$120.77
733	0167463530000	$120.77
734	0167463540000	$120.77
735	0167463550000	$120.77
736	0167463560000	$120.77
737	0167463570000	$120.77
738	0167463580000	$120.77
739	0167463590000	$120.77
740	0167463600000	$120.77
741	0167463610000	$120.77
742	0167463620000	$120.77
743	0167463630000	$120.77
744	0167463640000	$120.77
745	0167463650000	$120.77
746	0167463660000	$120.77
747	0167463670000	$120.77
748	0167463680000	$120.77
749	0167463690000	$120.77
750	0167473010000	$120.77
751	0167473020000	$120.77
752	0167473030000	$120.77
753	0167473040000	$120.77
754	0167473050000	$120.77
755	0167473060000	$120.77
756	0167473070000	$120.77
757	0167473080000	$120.77
758	0167473090000	$120.77

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
759	0167473100000	$120.77
760	0167473110000	$120.77
761	0167473120000	$120.77
762	0167473130000	$120.77
763	0167473140000	$120.77
764	0167473150000	$120.77
765	0167473160000	$120.77
766	0167473170000	$120.77
767	0167473180000	$120.77
768	0167473190000	$120.77
769	0167473200000	$120.77
770	0167473210000	$120.77
771	0167473220000	$120.77
772	0167473230000	$120.77
773	0167473240000	$120.77
774	0167473250000	$120.77
775	0167473260000	$120.77
776	0167473270000	$120.77
777	0167473280000	$120.77
778	0167473290000	$120.77
779	0167473300000	$120.77
780	0167473310000	$120.77
781	0167473320000	$120.77
782	0167473330000	$120.77
783	0167473340000	$120.77
784	0167473350000	$120.77
785	0167473360000	$120.77
786	0167473370000	$120.77
787	0167473380000	$120.77
788	0167473390000	$120.77
789	0167473400000	$120.77
790	0167473410000	$120.77
791	0167473420000	$120.77
792	0167473430000	$120.77
793	0167473440000	$120.77
794	0167473450000	$120.77
795	0167473460000	$120.77
796	0167473470000	$120.77
797	0167473480000	$120.77
798	0167473490000	$120.77
799	0167473500000	$120.77
800	0167473510000	$120.77
801	0167473520000	$120.77
802	0167473530000	$120.77
803	0167473540000	$120.77
804	0167473550000	$120.77
805	0167473560000	$120.77
806	0167473570000	$120.77
807	0167473580000	$120.77
808	0167473590000	$120.77
809	0167473600000	$120.77
810	0167473610000	$120.77
811	0167473620000	$120.77
812	0167473630000	$120.77
813	0167473640000	$120.77

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy	
814	0167473650000	$120.77	
815	0167473660000	$120.77	
816	0167473670000	$120.77	
817	0167473680000	$120.77	
818	0167473690000	$120.77	
819	0167474010000	$120.77	
820	0167474020000	$120.77	
821	0167474030000	$120.77	
822	0167474040000	$120.77	
823	0167474050000	$120.77	
824	0167474060000	$120.77	
825	0167474070000	$120.77	
826	0167474080000	$120.77	
827	0167474090000	$120.77	
828	0167474100000	$120.77	
829	0167474110000	$120.77	
830	0167474120000	$120.77	
831	0167474130000	$120.77	
832	0167474140000	$120.77	
833	0167474150000	$120.77	
834	0167474160000	$120.77	
835	0167474170000	$120.77	
836	0167474180000	$120.77	
837	0167474190000	$120.77	
838	0167474200000	$120.77	
839	0167474210000	$120.77	
840	0167474220000	$120.77	
841	0167474230000	$120.77	
842	0167474240000	$120.77	
843	0167474250000	$120.77	
844	0167474260000	$120.77	
845	0167474270000	$120.77	
846	0167474280000	$120.77	
847	0167474290000	$120.77	
848	0167474300000	$120.77	
849	0167474310000	$120.77	
850	0167474320000	$120.77	
851	0167474330000	$120.77	
852	0167474340000	$120.77	
853	0167474350000	$120.77	
854	0167474360000	$120.77	
855	0167474370000	$120.77	
856	0167474380000	$120.77	
857	0292032310000	$167.26	Annex No. 27
858	0292032360000	$3.32	
859	0292032480000	$4,829.57	
860	0167931010000	$410.09	Annex No. 29
861	0167931020000	$410.09	
862	0167931030000	$410.09	
863	0167931040000	$410.09	
864	0167931050000	$410.09	
865	0167931060000	$410.09	
866	0167931070000	$410.09	
867	0167931080000	$410.09	
868	0167931090000	$410.09	

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
869	0167931100000	$410.09
870	0167931110000	$410.09
871	0167931120000	$410.09
872	0167931130000	$410.09
873	0167931140000	$410.09
874	0167931150000	$410.09
875	0167931160000	$410.09
876	0167931170000	$410.09
877	0167931180000	$410.09
878	0167931190000	$410.09
879	0167931200000	$410.09
880	0167931210000	$410.09
881	0167931220000	$410.09
882	0167931230000	$410.09
883	0167931240000	$410.09
884	0167931250000	$410.09
885	0167931260000	$410.09
886	0167931270000	$410.09
887	0167931280000	$410.09
888	0167931290000	$410.09
889	0167931300000	$410.09
890	0167931310000	$410.09
891	0167931320000	$410.09
892	0167931330000	$410.09
893	0167931340000	$410.09
894	0167931350000	$410.09
895	0167931360000	$410.09
896	0167931370000	$410.09
897	0167931380000	$410.09
898	0167931390000	$410.09
899	0167931400000	$410.09
900	0167931410000	$410.09
901	0167931420000	$410.09
902	0167931430000	$410.09
903	0167931440000	$410.09
904	0167931450000	$410.09
905	0167932010000	$410.09
906	0167932020000	$410.09
907	0167932030000	$410.09
908	0167932040000	$410.09
909	0167932050000	$410.09
910	0167932060000	$410.09
911	0167932070000	$410.09
912	0167932080000	$410.09
913	0167932090000	$410.09
914	0167932100000	$410.09
915	0167932110000	$410.09
916	0167932120000	$410.09
917	0167932130000	$410.09
918	0167932140000	$410.09
919	0167932150000	$410.09
920	0167932160000	$410.09
921	0167932170000	$410.09
922	0167932180000	$410.09
923	0167932190000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
924	0167932200000	$410.09
925	0167932210000	$410.09
926	0167932220000	$410.09
927	0167932230000	$410.09
928	0167932240000	$410.09
929	0167932250000	$410.09
930	0167932260000	$410.09
931	0167932270000	$410.09
932	0167932280000	$410.09
933	0167932290000	$410.09
934	0167932300000	$410.09
935	0167932310000	$410.09
936	0167932320000	$410.09
937	0167932330000	$410.09
938	0167932340000	$410.09
939	0167932350000	$410.09
940	0167932360000	$410.09
941	0167932370000	$410.09
942	0167932380000	$410.09
943	0167932390000	$410.09
944	0167932400000	$410.09
945	0167932410000	$410.09
946	0167932420000	$410.09
947	0167932430000	$410.09
948	0167932440000	$410.09
949	0167932450000	$410.09
950	0167932460000	$410.09
951	0167932470000	$410.09
952	0167932480000	$410.09
953	0167932490000	$410.09
954	0167932500000	$410.09
955	0167932510000	$410.09
956	0167932520000	$410.09
957	0167932530000	$410.09
958	0167932540000	$410.09
959	0167941010000	$410.09
960	0167941020000	$410.09
961	0167941030000	$410.09
962	0167941040000	$410.09
963	0167941050000	$410.09
964	0167941060000	$410.09
965	0167941070000	$410.09
966	0167941080000	$410.09
967	0167941090000	$410.09
968	0167941100000	$410.09
969	0167941110000	$410.09
970	0167941120000	$410.09
971	0167941130000	$410.09
972	0167941140000	$410.09
973	0167941150000	$410.09
974	0167941160000	$410.09
975	0167941170000	$410.09
976	0167941180000	$410.09
977	0167941190000	$410.09
978	0167941200000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
979	0167941210000	$410.09
980	0167941220000	$410.09
981	0167941230000	$410.09
982	0167941240000	$410.09
983	0167941250000	$410.09
984	0167941260000	$410.09
985	0167941270000	$410.09
986	0167941280000	$410.09
987	0167941290000	$410.09
988	0167941300000	$410.09
989	0167941310000	$410.09
990	0167941320000	$410.09
991	0167941330000	$410.09
992	0167941340000	$410.09
993	0167951010000	$410.09
994	0167951020000	$410.09
995	0167951030000	$410.09
996	0167951040000	$410.09
997	0167951050000	$410.09
998	0167951060000	$410.09
999	0167951070000	$410.09
1000	0167951080000	$410.09
1001	0167951090000	$410.09
1002	0167951100000	$410.09
1003	0167951110000	$410.09
1004	0167951120000	$410.09
1005	0167951130000	$410.09
1006	0167951140000	$410.09
1007	0167951150000	$410.09
1008	0167951160000	$410.09
1009	0167951170000	$410.09
1010	0167951180000	$410.09
1011	0167951190000	$410.09
1012	0167951200000	$410.09
1013	0167951210000	$410.09
1014	0167951220000	$410.09
1015	0167951230000	$410.09
1016	0167951240000	$410.09
1017	0167951250000	$410.09
1018	0167951260000	$410.09
1019	0167951270000	$410.09
1020	0167951280000	$410.09
1021	0167951290000	$410.09
1022	0167951300000	$410.09
1023	0167951310000	$410.09
1024	0167951320000	$410.09
1025	0167951330000	$410.09
1026	0167951340000	$410.09
1027	0167951350000	$410.09
1028	0167951360000	$410.09
1029	0167951370000	$410.09
1030	0167951380000	$410.09
1031	0167951390000	$410.09
1032	0167951400000	$410.09
1033	0167951410000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1034	0167951420000	$410.09
1035	0167951430000	$410.09
1036	0167951440000	$410.09
1037	0167951450000	$410.09
1038	0167951460000	$410.09
1039	0167951470000	$410.09
1040	0167951480000	$410.09
1041	0167951490000	$410.09
1042	0167951500000	$410.09
1043	0167951510000	$410.09
1044	0167951520000	$410.09
1045	0167951530000	$410.09
1046	0167951540000	$410.09
1047	0167951550000	$410.09
1048	0167951560000	$410.09
1049	0167951570000	$410.09
1050	0167951580000	$410.09
1051	0167951590000	$410.09
1052	0167951600000	$410.09
1053	0167951610000	$410.09
1054	0167951620000	$410.09
1055	0167951630000	$410.09
1056	0167961010000	$410.09
1057	0167961020000	$410.09
1058	0167961030000	$410.09
1059	0167961040000	$410.09
1060	0167961050000	$410.09
1061	0167961060000	$410.09
1062	0167961070000	$410.09
1063	0167961080000	$410.09
1064	0167961090000	$410.09
1065	0167961100000	$410.09
1066	0167961110000	$410.09
1067	0167961120000	$410.09
1068	0167961130000	$410.09
1069	0167961140000	$410.09
1070	0167961150000	$410.09
1071	0167961160000	$410.09
1072	0167961170000	$410.09
1073	0167961180000	$410.09
1074	0167961190000	$410.09
1075	0167961200000	$410.09
1076	0167961210000	$410.09
1077	0167961220000	$410.09
1078	0167961230000	$410.09
1079	0167961240000	$410.09
1080	0167961250000	$410.09
1081	0167961260000	$410.09
1082	0167961270000	$410.09
1083	0167961280000	$410.09
1084	0167961290000	$410.09
1085	0167961300000	$410.09
1086	0167961310000	$410.09
1087	0167961320000	$410.09
1088	0167961330000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1089	0167961340000	$410.09
1090	0167961350000	$410.09
1091	0167961360000	$410.09
1092	0167961370000	$410.09
1093	0167961380000	$410.09
1094	0167961390000	$410.09
1095	0167961400000	$410.09
1096	0167961410000	$410.09
1097	0167961420000	$410.09
1098	0167961430000	$410.09
1099	0167961440000	$410.09
1100	0167961450000	$410.09
1101	0167961460000	$410.09
1102	0167961470000	$410.09
1103	0167961480000	$410.09
1104	0167962010000	$410.09
1105	0167962020000	$410.09
1106	0167962030000	$410.09
1107	0167962040000	$410.09
1108	0167962050000	$410.09
1109	0167962060000	$410.09
1110	0167962070000	$410.09
1111	0167962080000	$410.09
1112	0167962090000	$410.09
1113	0167962100000	$410.09
1114	0167962110000	$410.09
1115	0167962120000	$410.09
1116	0167962130000	$410.09
1117	0167962140000	$410.09
1118	0167962150000	$410.09
1119	0167962160000	$410.09
1120	0167962170000	$410.09
1121	0167962180000	$410.09
1122	0167962190000	$410.09
1123	0167962200000	$410.09
1124	0167962210000	$410.09
1125	0167962220000	$410.09
1126	0167962230000	$410.09
1127	0167962240000	$410.09
1128	0167962250000	$410.09
1129	0167962260000	$410.09
1130	0167962270000	$410.09
1131	0167962280000	$410.09
1132	0167962290000	$410.09
1133	0167962300000	$410.09
1134	0167962310000	$410.09
1135	0167962320000	$410.09
1136	0167962330000	$410.09
1137	0167962340000	$410.09
1138	0167962350000	$410.09
1139	0167962360000	$410.09
1140	0167962370000	$410.09
1141	0167962380000	$410.09
1142	0167962390000	$410.09
1143	0167962400000	$410.09

EXHIBIT "A"

ANNEXATION LEVY SUMMARY

City of Redlands

Community Facilities District No. 2004-1

Fiscal Year 2026-2027 Special Tax Levy

Line No.	Assessor's Parcel No.	Special Tax Levy
1144	0167962410000	$410.09
1145	0167962420000	$410.09
1146	0167962430000	$410.09
1147	0167962440000	$410.09
1148	0167962450000	$410.09
1149	0167962460000	$410.09
1150	0167962470000	$410.09
1151	0167962480000	$410.09
1152	0167962490000	$410.09
1153	0167962500000	$410.09
1154	0167962510000	$410.09
1155	0167962520000	$410.09
1156	0167962530000	$410.09
1157	0167962540000	$410.09
1158	0167962550000	$410.09
1159	0167962560000	$410.09
1160	0167962570000	$410.09
1161	0167962580000	$410.09
1162	0167962590000	$410.09
1163	0167962600000	$410.09
1164	0167962610000	$410.09
1165	0167962620000	$410.09
1166	0167962630000	$410.09
1167	0167962640000	$410.09
1168	0167962650000	$410.09
1169	0167962660000	$410.09
1170	0167962670000	$410.09
1171	0167962680000	$410.09
1172	0167962690000	$410.09
1173	0167962700000	$410.09
1174	0167962710000	$410.09
1175	0167962720000	$410.09
1176	0167962730000	$410.09
1176 Parcels	**Totals**	**$930,997.38**

EXHIBIT "B"
CITY OF REDLANDS
CFD 2004-1

District Landscaping	Maintenance Category	Tract/ Parcel Map No.	Landscape Areas	BUs	FY 26-27 Maximum Rates per Benefit Unit [1]	FY 26-27 Maximum Total Assessment	FY 26-27 Applied Rates per Benefit Unit	FY 26-27 Total Levy per Annexation [2]	FY 26-27 Percent of Max Tax
CFD 2004-1 Orig.	K	TR 16408	Please see Orig. ER	64.00	3.09% inc. $2,492.16	$159,498.37	$1,953.13	$125,000.00	78.37%
Annexation 1	B	TR 16287	Drainage Basin	12.00	3.09% inc. $641.65	$7,699.77	$491.67	$5,900.00	76.63%
Annexation 2	On Hold	TR 16586		n/a	n/a	n/a	n/a	n/a	n/a
Annexation 3	A (Construction has not started)	TTM 17253		37.00	3.09% inc. $427.35	$15,812.09	$0.00	$0.00	0.00%
Annexation 4	0	PM 17353	Ford Street Median	5.80	3.09% inc. $2,765.23	$16,038.34	$2,275.86	$13,200.00	82.30%
Annexation 5	E	CRA 826	California Street center Median	11.75	3.09% inc. $1,089.33	$12,799.67	$885.11	$10,400.00	81.25%
Annexation 6	Failed	TR 14790-1		n/a	n/a	n/a	n/a	n/a	n/a
Annexation 7	On Hold	Parcel 2 of PM 15573		n/a	n/a	n/a	n/a	n/a	n/a
Annexation 8	A (Construction has not started)	TTM 16806		6.00	3.09% inc. $411.32	$2,467.94	$0.00	$0.00	0.00%
Annexation 9	A	PM 18208	Redlands Median	42.55	3.09% inc. $383.76	$16,329.04	$331.37	$14,100.00	86.35%
Annexation 10	On Hold	TR 18762		n/a	n/a	n/a	n/a	n/a	n/a
Annexation 11	A (BOA Maintained)	PM 19371	Street Trees on Lugonia & Wabash	39.90	3.09% inc. $368.86	$14,717.48	$0.00	$0.00	0.00%
Annexation 12a	G	TR 16465	Street trees, parkways, basin, proposed Orange groves	61.00	3.09% inc. $1,197.40	$73,041.23	$1,052.46	$64,200.00	87.90%
Annexation 12b	H	TR 16627	Street trees, parkways, basin, proposed Orange groves	20.00	3.09% inc. $1,338.27	$26,765.35	$1,185.00	$23,700.00	88.55%
Annexation 12c	G	TR 18979, 19975 & 20079	Street trees, parkways, basin, proposed Orange groves	122.00	3.09% inc. $1,197.40	$146,082.45	$1,065.57	$130,000.00	88.99%
Annexation 12d	G	TR 18979, 19975 & 20079	Street trees, parkways, basin, proposed Orange groves	14.00	3.09% inc. $1,197.40	$16,763.56	$1,071.43	$15,000.00	89.48%
Annexation 13	M (HOA Maintained)	TR 18882	Street Trees	26.00	3.09% inc. $2,182.12	$56,735.05	$0.00	$0.00	0.00%
Annexation 14	A	Planned Dev. # 1 PM 19496	California Median Owner to maintain Parkways	71.18	3.09% inc. $361.63	$25,740.59	$140.49	$10,000.00	38.85%
Annexation 15	A	PM 18536-1	Ground cover, shrubs, turf, trees and palm trees	50.50	3.09% inc. $328.31	$16,579.49	$0.00	$0.00	0.00%
Annexation 16	I	TR 18988	Riverview & Texas St.- Parks, slopes, parkways, median, open space, seating and monument structures	82.00	3.09% inc. $1,450.13	$118,911.07	$1,317.07	$108,000.00	90.82%
Annexation 17	H	TR 17022	Ground cover, shrubs, citrus and palm trees	12.00	3.09% inc. $1,334.17	$16,010.02	$0.00	$0.00	0.00%
Annexation 18	E (Owner Maintained)	PM 19465	Ground cover, shrubs, turf, trees and palm trees	17.80	3.09% inc. $897.70	$15,979.11	$0.00	$0.00	0.00%
Annexation 19	J	TTM 19942	Sylvan Blvd & Wabash St.- Mulch, shrubs, trees, orange groves, trees and palm trees	34.00	3.09% inc. $1,510.21	$51,347.16	$1,352.94	$46,000.00	89.59%
Annexation 20	H	TTM 19956	Highland Ave. & Wabash St.- Ground cover, shrubs, turf, trees and palm trees	40.00	3.09% inc. $1,276.30	$51,052.17	$1,150.00	$46,000.00	90.10%
Annexation 21	J	TR 20126	Judson St & Lugonia Ave.- Ground cover, mulch, shrubs, orange groves, trees and basin	105.00	3.09% inc. $1,545.00	$162,224.99	$1,380.95	$145,000.00	89.38%
Annexation 22	A (Owner Maintained)	PM 19981 CRA 900	Parkway	15.48	3.09% inc. $328.31	$5,082.19	$0.00	$0.00	0.00%
Annexation 23	B	PM 18536	Parkway	9.55	3.09% inc. $443.81	$4,238.41	$0.00	$0.00	0.00%
Annexation 24	E	CUP 1129	Parkway	3.95	3.09% inc. $824.22	$3,255.68	$0.00	$0.00	0.00%
Annexation 25	G	TTM 20065	Moore St, Lot A, infiltration nasin, trenches, storm drain facilities, and street trees	29.00	3.09% inc. $936.67	$27,163.31	$500.00	$14,500.00	53.38%

EXHIBIT "B"
CITY OF REDLANDS
CFD 2004-1

District Landscaping	Maintenance Category	Tract/ Parcel Map No.	Landscape Areas	BUs	FY 26-27 Maximum Rates per Benefit Unit [1]	FY 26-27 Maximum Total Assessment	FY 26-27 Applied Rates per Benefit Unit	FY 26-27 Total Levy per Annexation [2]	FY 26-27 Percent of Max Tax
Annexation 26	B	TR 20257	Texas & Pioneer - Parkway trees	207.00	3.09% inc. $403.31	$83,484.76	$120.77	$25,000.00	29.95%
Annexation 27	A	Mountain View Building Planned Dev. #4	Split Rail Fence & Concrete	45.14	3.09% inc. $288.08	$13,003.80	$110.77	$5,000.00	38.45%
Annexation 28	C	TR 20473	Parkway Trees	98.00	$450.00	$44,100.00	$0.00	$0.00	0.00%
Annexation 29	D	TR 20336	Parkways, Sports Park, and drainage basins	317.00	3.09% inc. $581.33	$184,281.13	$410.09	$130,000.00	70.54%
Annexation 30	B	TR 20528	Parkways, Contech Diversion Structureand biofileration system	117.00	$350.00	$40,950.00	$0.00	$0.00	0.00%
							Total	$931,000.00	

[1] The percentage increase listed is rounded to two decimal places, but has not been rounded when calculating the maximum rates for Fiscal Year 2026-27.

[2] Amount may be slightly off due to rounding.

Max/Applied Tax Rates per Benefit Unit for FY 26-27

District	Max Rates	Applied Rates	Notes
Original District (TR 16408)	$2,492.16	$1,953.13	
Annexation No. 1 (TR 16287)	$641.65	$491.67	
Annexation No. 2 (TR 16586)	n/a	n/a	Annexation is on Hold
Annexation No. 3 (TTM 17253)	$427.35	$0.00	
Annexation No. 4 (PM 17353)	$2,765.23	$2,275.86	
Annexation No. 5 (CRA 826)	$1,089.33	$885.11	
Annexation No. 6 (TR 14790-1)	n/a	n/a	Annexation Failed
Annexation No. 7 (PM 15573)	n/a	n/a	Annexation is on Hold
Annexation No. 8 (TR 16806)	$411.32	$0.00	
Annexation No. 9 (PM 18208)	$383.76	$331.37	
Annexation No. 10 (TR 18762)	n/a	n/a	Annexation is on Hold
Annexation No. 11 (PM 19731)	$368.86	$0.00	Business Owner's Association maintained.
Annexation No. 12a (TR 16465)	$1,197.40	$1,052.46	
Annexation No. 12b (TR 16627)	$1,338.27	$1,185.00	
Annexation No. 12c (TR 18979, 19975 & 20079)	$1,197.40	$1,065.57	
Annexation No. 12d (TR 18979, 19975 & 20079)	$1,197.40	$1,071.43	
Annexation No. 13 (TR 18882)	$2,182.12	$0.00	HOA Maintained
Annexation No. 14 (PM 19496)	$361.63	$140.49	
Annexation No. 15 (PM 18536-1)	$328.31	$0.00	
Annexation No. 16 (TR 18988)	$1,450.13	$1,317.07	
Annexation No. 17 (TR 17022)	$1,334.17	$0.00	
Annexation No. 18 (PM 19465)	$897.70	$0.00	Owner Maintained
Annexation No. 19 (PM 19942)	$1,510.21	$1,352.94	
Annexation No. 20 (TM 19956)	$1,276.30	$1,150.00	
Annexation No. 21 (TR 20126)	$1,545.00	$1,380.95	
Annexation No. 22 (PM 19981 CRA 900)	$328.31	$0.00	Owner Maintained
Annexation No. 23 (PM 18536)	$443.81	$0.00	
Annexation No. 24 (CUP 1129)	$824.22	$0.00	
Annexation No. 25 (TTM 20065)	$936.67	$500.00	
Annexation No. 26 (TR20257)	$403.31	$120.77	
Annexation No. 27 (Planned Dev #4)	$288.08	$110.77	
Annexation No. 28 (TR 20473)	$450.00	$0.00	
Annexation No. 29 (TR 20036)	$581.33	$410.09	
Annexation No. 30 (TR 20528)	$350.00	$0.00	

City Council **AGENDA ITEM NO. J1.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Conference Report- 2026 League of California Cities Annual Conference and Expo (Mayor Saucedo)

DISCUSSION:

Mayor Saucedo , Mayor Pro Tem Shaw and Council Member Davis will provide reports relating to their attendance at the 2026 League of California Cities Annual Conference and Expo held September 23-25, 2026 in Anaheim, California.

City Council **AGENDA ITEM NO. J2.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Adopt Resolution No. 8834 supporting Proposition 1, the Veterans and Affordable Housing Bond Act of 2026, which authorizes $11.25 billion in state general obligation bonds to fund several housing affordability programs (Mayor Saucedo)

MOTION:

If the City Council determines that the Mayor's recommendation is appropriate, the following motion is provided:

I move to adopt Resolution No. 8834 supporting Proposition 1, the Veterans and Affordable Housing Bond Act of 2026.

RECOMMENDATION:

The Mayor recommends that the City Council adopt Resolution No. 8834 supporting Proposition 1, the Veterans and Affordable Housing Bond Act of 2026, which authorizes $11.25 billion in state general obligation bonds to fund several housing affordability programs.

DISCUSSION:

The Veterans and Affordable Housing Bond Act of 2026 would authorize the state to issue $11.25 billion in general obligation bonds to fund several categories of existing housing programs, including:

- Multifamily Housing Program
- Infill Infrastructure Grant Program
- CalHome Program
- Farmworker Housing
- Tribal Housing Grant Program
- Higher Education student housing
- Local pilot programs
- Veterans' Housing

Major Provisions:

The Veterans and Affordable Housing Bond Act of 2026 is a measure placed on the November 3, 2026 ballot by the Legislature that would replenish existing housing programs for the development, preservation, and rehabilitation of affordable housing projects. Additionally, the measure would provide funding to support the development of youth and veteran housing and promote home ownership in California. Here are the specific funding allocations proposed in the ballot measure:

- $5.1 billion to the Multifamily Housing Program.

- $1.25 billion to provide farm and home aid for veterans under the Veterans' Farm and Home Purchase Act of 1974.
- $1.15 billion to the Housing Rehabilitation Loan Fund, to be used for supportive housing. Up to 15% shall be used to assist in the acquisition, conversion, or rehabilitation of interim housing to permanent housing.
- $750 million to the Portfolio Reinvestment Program to preserve existing affordable housing projects.
- $600 million to the CalHome Program.
- $500 million to the Home Purchase Assistance Fund for home purchase assistance programs.
- $500 million for the Infill Infrastructure Grant Program to assist in the construction and rehabilitation of infrastructure to support high-density, affordable, and mixed-income housing in infill locations.
- $450 million to the Joe Serna, Jr. Farmworker Housing Grant Fund to support housing for agricultural employees and their families.
- $350 million for new affordable student housing projects.
- $200 million to fund the acquisition and rehabilitation of unrestricted housing units and attach long-term affordability restrictions on housing units.
- $200 million to the Affordable Housing Innovation Fund to assist local housing trust funds in developing, owning, lending, or investing in affordable housing.
- $200 million to the Tribal Housing Grant Program to help tribes rebuild and reconstitute their communities.
- $150 million for youth housing defined as housing for current or former foster youth, homeless minors or youth, or youth at risk of homelessness.

Background:

The state uses general obligation bonds to fund various housing programs. Bonds are a way the state borrows money to cover the up-front costs of a development and then repays the money plus interest over time.

Proposition 1 would allow the state to sell $11.25 billion in general obligation bonds for housing purposes. This amount consists of (1) a $10 billion bond for a variety of housing programs that would be repaid by the State's General Fund and (2) a $1.25 billion bond that would be repaid by veterans' payments on their home loans.

According to the nonpartisan Legislative Analyst's Office, Prop. 1 would provide subsidies for as many as 40,000 multifamily rental units and about 1,200 beds for university students. The funds could also help up to 40,000 households, including about 2,100 veterans, with homeownership.

Arguments in Support:

Proponents of the measure argue that it gives Californians the opportunity to provide housing to working families, veterans, people with disabilities and seniors; helps prevent homelessness by keeping vulnerable persons in their homes; expands homeownership opportunities; and maintains strict fiscal accountability and transparency without new taxes. Proponents also argue that it would jumpstart the construction of tens of thousands of shovel-ready affordable homes across California.

The League of California Cities, which has long supported investments that increase the supply of affordable housing, also supports Prop. 1. Cal Cities maintains that, if approved by the voters, Prop. 1 would replenish funding for several successful state programs used by cities to support affordable housing and infrastructure. Prop. 1 could also fund innovative local programs like regional housing trusts and support cities in meeting their Regional Housing Need Assessment (RHNA) goals for current and future cycles.

In addition to funding new affordable housing projects, the measure would fund the rehabilitation and preservation of existing affordable housing, increase funding for homeownership programs, and support specific housing projects — such as student housing, infill development, supportive housing, and foster youth housing.

No argument against Proposition 1 was submitted to the California Secretary of State.

The City of Redlands continues to have a need for additional affordable housing, particularly for seniors and veterans living on fixed or limited incomes. Rising housing costs and limited affordable units can increase the risk of housing instability and homelessness. Expanding affordable housing opportunities for these populations will support long-term housing stability, provide better access to supportive services, and strengthen the City's ongoing efforts to prevent and reduce homelessness.

ALTERNATIVES:

The City Council may choose not to adopt Resolution No. 8834.

STRATEGIC PLAN:
N/A

SUBMITTED BY:
Mario Saucedo, Mayor

REVIEWED BY:
Charles M. Duggan Jr., City Manager
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Whitney Mesna, Management Analyst

FISCAL IMPACT

Fiscal Year: N/A

Revenue Generating: No

Amount: $0

Budgeted Y/N: N/A

Account No.: N/A

Additional Appropriation Required: No

Discussion:

There is no fiscal impact associated with the adoption of this resolution.

Attachments

Resolution_No_8834_Support_of_Prop_1.pdf

RESOLUTION NO. 8834

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS IN SUPPORT OF PROPOSITION 1: THE VETERANS AND AFFORDABLE HOUSING BOND ACT OF 2026

WHEREAS, Cal Cities and its member cities advocate for secure investments to increase the supply of affordable housing; and

WHEREAS, Proposition 1, the Veterans and Affordable Housing Bond Act of 2026, will appear on the November 3, 2026, statewide ballot and authorize the state to issue $11.25 billion in state general obligation bonds to provide funding to build and preserve affordable homes and expand homeownership opportunities across California; and

WHEREAS, Proposition 1 is anticipated to provide funding to fast-track numerous already-approved, shovel-ready affordable homes, turning stalled projects into homes for families who need them; and

WHEREAS, Proposition 1 is anticipated to provide funding to build homes working families can afford, so that the teachers, firefighters, and nurses who serve the City of Redlands can afford to live in the community they serve; and

WHEREAS, Proposition 1 honors our veterans by dedicating $1.25 billion solely to veterans' housing and homeownership opportunities, including the CalVet Home Loan Program, which has already helped almost a million veterans and their families; and

WHEREAS, Proposition 1 helps our most vulnerable neighbors by providing funding to create and preserve housing for low-income residents, seniors, those who are homeless or at risk of homelessness, foster youth experiencing homelessness, and people with disabilities; and

WHEREAS, Proposition 1 does not raise taxes, but may unlock matching federal funds, bringing tax dollars Californians send to Washington back home to California; and

WHEREAS, Proposition 1 comes with strict accountability, public reporting, and clear requirements, so that voters can see how many homes get built, where, and at what cost; and

WHEREAS, Proposition 1 benefits veterans, seniors, low- and middle-income Californians, persons with disabilities, working families, farmworkers, students, first-time homebuyers, and our youth; and

WHEREAS, the City Council of Redlands finds that the safe, affordable homes and veteran housing investments made possible by Proposition 1 are in the best interest of the residents of the City of Redlands;

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF REDLANDS AS FOLLOWS:

Section 1. The City Council of the City of Redlands supports Proposition 1, the Veterans and Affordable Housing Bond Act of 2026.

Section 2. This Resolution shall become effective immediately upon its adoption.

ADOPTED, SIGNED AND APPROVED this 6th day of October, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, hereby certify that the foregoing resolution was duly adopted by the City Council at a regular meeting thereof held on the 6th day of October, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. J3.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Discussion and possible action to approve Resolution No. 8837 amending the procedures and guidelines for reviewing applications to fill vacancies on the Planning Commission and rescinding Resolution No. 8674 (Mayor Pro Tem Shaw)

MOTION:

If the City Council determines that Mayor Pro Tem's recommendation is appropriate, the following motion is provided:

I move to approve Resolution No. 8837 amending the procedures and guidelines for reviewing applications to fill vacancies on the Planning Commission and rescinding Resolution No. 8674.

RECOMMENDATION:

Mayor Pro Tem Shaw recommends that the City Council approve Resolution No. 8837 amending the procedures and guidelines for reviewing applications to fill vacancies on the Planning Commission and rescinding Resolution No. 8674.

DISCUSSION:

On April 15, 2025, the City Council adopted Resolution No. 8674 establishing procedures and guidelines for reviewing applications to fill vacancies on the Planning Commission. The procedures include the formation of a two-member City Council ad hoc subcommittee to review applications and make recommendations to the City Council.

Resolution No. 8674 currently requires the ad hoc subcommittee to interview all finalists prior to making its recommendations. The proposed Resolution would amend this requirement to make finalist interviews optional, allowing the ad hoc subcommittee to determine whether interviews are necessary. All other procedures and guidelines would remain unchanged.

The proposed Resolution does not require environmental review pursuant to Sections 15061(b)(3) and 15378(b)(5) of the California Environmental Quality Act Guidelines because this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment.

ALTERNATIVES:

The City Council may choose not to approve the proposed Resolution and retain the current procedures and guidelines.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Mayor Pro Tem Shaw

REVIEWED BY:
Charles M. Duggan Jr., City Manager
Yvette M. Abich Garcia, City Attorney

PREPARED BY:
Whitney Mesna, Management Analyst

FISCAL IMPACT

Fiscal Year: 2026-27

Revenue Generating: No

Amount: N/A

Budgeted Y/N:

Account No.:

Additional Appropriation Required: Yes or No

Discussion:

There is no fiscal impact associated with the adoption of the proposed Resolution.

Attachments

Resolution_No_8837_Planning_Commission.pdf
8674_Planning_Commission_Vacancies.pdf
Resolution-_Redline.pdf

RESOLUTION NO. 8837

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS AMENDING THE PROCEDURES AND GUIDELINES FOR REVIEWING APPLICATIONS TO FILL VACANCIES ON THE PLANNING COMMISSION.

WHEREAS, in April 2025, the Redlands City Council enacted procedures and guidelines for reviewing applications and filling vacancies on the Redlands Planning Commission; and

WHEREAS, the Redlands City Council now wish to amend the appointment procedure for the Planning Commission by requiring finalist interviews by the ad hoc subcommittee to be optional and not mandatory; and

WHEREAS, the adoption of this Resolution qualifies for exemption from environmental review in accordance with Sections 15061(b)(3) and 15378(b)(5) of the California Environmental Quality Act.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF REDLANDS AS FOLLOWS:

Section 1. Procedures and Guidelines to Fill Vacancies on the Planning Commission. The following procedures and guidelines are hereby adopted pertaining to the review of applications and recommendations to the City Council to fill vacancies on the Planning Commission:

I. City Council Ad Hoc Subcommittee

I. The Mayor shall appoint an ad hoc subcommittee at a regularly scheduled City Council meeting, and said committee shall consist of two (2) Councilmembers, with approval of a majority of Councilmembers present.

2. The notice of vacancy shall be posted by the City Clerk in accordance with State law.

3. The ad hoc subcommittee shall review all complete applications that are received prior to the published date and time deadline for a commission vacancy. Applicants may not submit additional information after the filing deadline, nor may members of the ad hoc subcommittee or City staff request additional information or materials after the filing deadline.

4. The ad hoc subcommittee shall report its findings and recommendations to the City Council in a regular public City Council meeting. Consensus by the ad hoc subcommittee is not required for consideration of an applicant by the full City Council.

5. The ad hoc subcommittee shall be automatically disbanded (without further action required by the City Council) upon the appointment(s) of new Commissioner(s) and all vacancies on the Planning Commission have been filled.

II. Criteria for Review of Applications

1. Eligible applicants shall be residents of the City of Redlands and registered to vote at the time of filing the application. Councilmembers may consider the applicant's length of residency as well as knowledge of local planning or community development trends and issues.

2. Councilmembers shall consider the applicant's background, training, and/or professional experience and its relevance to the Planning Commission's duties and responsibilities. Preference will be given to applicants who have knowledge, training, and/or experience that are directly related to and will contribute meaningfully to the Planning Commission's responsibilities. Relevant fields of knowledge, training, or experience include, but are not limited to, urban planning, architecture, civil engineering, landscape architecture, real estate, real estate development, community development, economic development, environmental policy, public policy, public administration, finance and business administration.

3. Councilmembers may also consider other relevant factors such as: the applicant's demonstrated history of civic involvement in Redlands; previous positions and performance on other City of Redlands boards, commissions, or committees; or other volunteer or civic experience, and its relevance to the Planning Commission's duties and responsibilities.

4. Special consideration should be given to achieving a variety or diversity of backgrounds and representation on the Planning Commission, as this will contribute to a more fully informed analysis and public deliberation of topics by the entire Planning Commission.

5. Ad hoc subcommittee members may personally interview all finalists prior to making its recommendation(s) to the City Council.

III. Planning Commissioner Training

1. Planning Commissioners must maintain compliance with certain public official training requirements, including completing training courses for ethics and sexual harassment prevention.

2. The Development Services Department will provide introductory training for new Commissioners as soon as practicable after appointment.

3. The Development Services Department will provide relevant training for all Commissioners on an annual or as-needed basis. Commissioners may obtain training from external providers or conferences, with registration costs (including costs for any books or related course materials) paid by the City, subject to budget availability and pre-authorization by the Development Services Director.

Section 2. California Environmental Quality Act. The proposed Resolution does not require environmental review in accordance with Sections 1506l(b)(3) and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section l5378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the adoption of the Resolution may have a significant effect on the environment, insofar as it would establish administrative procedures and guidelines for reviewing applications to fill vacancies on the City of Redlands Planning Commission.

Section 3. Resolution No. 8674 is hereby rescinded.

Section 4. Effective Date. This Resolution shall take effect upon adoption.

ADOPTED, SIGNED AND APPROVED this 6th day of October, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, CityClerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, do hereby certify that the foregoing Resolution was duly adopted by the City Council at a regular meeting thereof held on the 6th day of October, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

RESOLUTION NO. 8674

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS ESTABLISHING PROCEDURES AND GUIDELINES FOR REVIEWING APPLICATIONS TO FILL VACANCIES ON THE PLANNING COMMISSION.

WHEREAS, the Redlands City Council wishes to update its procedures for reviewing applications and filling vacancies on the Redlands Planning Commission; and

WHEREAS, the Redlands City Council has considered an ordinance updating Chapter 2.36 of Title 2 of the Redlands Municipal Code to amend the appointment procedure for the Planning Commission; and

WHEREAS, the adoption of Resolution No. 8674 qualifies for exemption from environmental review in accordance with Sections 15061(b)(3) and 15378(b)(5) of the California Environmental Quality Act.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF REDLANDS AS FOLLOWS:

Section 1. Procedures and Guidelines to Fill Vacancies on the Planning Commission. The following procedures and guidelines are hereby adopted pertaining to the review of applications and recommendations to the City Council to fill vacancies on the Planning Commission:

I. City Council Ad-Hoc Subcommittee

1. The Mayor shall appoint an ad-hoc subcommittee at a regularly scheduled City Council meeting, and said committee shall consist of two (2) Councilmembers, with approval of a majority of Councilmembers present.

2. The notice of vacancy shall be posted by the City Clerk in accordance with State law.

3. The ad-hoc subcommittee shall review all complete applications that are received prior to the published date and time deadline for a commission vacancy. Applicants may not submit additional information after the filing deadline, nor may members of the ad-hoc subcommittee or City staff request additional information or materials after the filing deadline.

4. The ad-hoc subcommittee shall report its findings and recommendations to the City Council in a regular public City Council meeting. Consensus by the ad-hoc subcommittee is not required for consideration of an applicant by the full City Council.

5. The ad-hoc subcommittee shall be automatically disbanded (without further action required by the City Council) upon the appointment(s) of new Commissioner(s) and all vacancies on the Planning Commission have been filled.

II. Criteria for Review of Applications

1. Eligible applicants shall be residents of the City of Redlands and registered to vote at the time of filing the application. Councilmembers may consider the applicant's length of residency as well as knowledge of local planning or community development trends and issues.

2. Councilmembers shall consider the applicant's background, training, and/or professional experience and its relevance to the Planning Commission's duties and responsibilities. Preference will be given to applicants who have knowledge, training, and/or experience that are directly related to and will contribute meaningfully to the Planning Commission's responsibilities. Relevant fields of knowledge, training, or experience include, but are not limited to, urban planning, architecture, civil engineering, landscape architecture, real estate, real estate development, community development, economic development, environmental policy, public policy, public administration, finance and business administration.

3. Councilmembers may also consider other relevant factors such as: the applicant's demonstrated history of civic involvement in Redlands; previous positions and performance on other City of Redlands boards, commissions, or committees; or other volunteer or civic experience, and its relevance to the Planning Commission's duties and responsibilities.

4. Special consideration should be given to achieving a variety or diversity of backgrounds and representation on the Planning Commission, as this will contribute to a more fully informed analysis and public deliberation of topics by the entire Planning Commission.

5. Ad hoc subcommittee members shall personally interview all finalists prior to making its recommendation(s) to the City Council.

III. Planning Commissioner Training

1. Planning Commissioners must maintain compliance with certain public official training requirements, including completing training courses for ethics and sexual harassment prevention.

2. The Development Services Department will provide introductory training for new Commissioners as soon as practicable after appointment.

3. The Development Services Department will provide relevant training for all Commissioners on an annual or as-needed basis. Commissioners may obtain training from external providers or conferences, with registration costs (including costs for any books or related course materials) paid by the City, subject to budget availability and pre-authorization by the Development Services Director.

Section 2. California Environmental Quality Act. The proposed Resolution does not require environmental review in accordance with Sections 15061(b)(3) and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the adoption of the Resolution may have a significant effect on the environment, insofar as it would establish administrative procedures and guidelines for reviewing applications to fill vacancies on the City of Redlands Planning Commission.

Section 3. Effective Date. This Resolution shall take effect upon adoption of Ordinance No. 2981.

ADOPTED, SIGNED AND APPROVED this 15th day of April, 2025.

Mario Saucedo, Mayor

ATTEST:

Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, do hereby certify that the foregoing Resolution was duly adopted by the City Council at a regular meeting thereof held on the 15th day of April, 2025, by the following vote:

AYES: Councilmembers Barich, Tejeda, Davis, Shaw; Mayor Saucedo
NOES:
ABSENT:
ABSTAIN:

Jeanne Donaldson, City Clerk

RESOLUTION NO. _____8674

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS AMENDINGESTABLISHING THE PROCEDURES AND GUIDELINES FOR REVIEWING APPLICATIONS TO FILL VACANCIES ON THE PLANNING COMMISSION.

WHEREAS, in April 2025, the Redlands City Council enacted procedures and guidelines for reviewing applications wishes to update its procedures for reviewing applications and filling vacancies on the Redlands Planning Commission; and

WHEREAS, the Redlands City Council now wish to amend the appointment procedure for the Planning Commission by requiring finalist interviews by the ad hoc subcommittee to be optional and not mandatoryhas considered an ordinance updating Chapter 2.36 of Title 2 of the Redlands Municipal Code to amend the appointment procedure for the Planning Commission; and

WHEREAS, the adoption of this Resolution No. 8674 qualifies for exemption from environmental review in accordance with Sections 15061(b)(3) and 15378(b)(5) of the California Environmental Quality Act.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF REDLANDS AS FOLLOWS:

Section I. Procedures and Guidelines to Fill Vacancies on the Planning Commission. The following procedures and guidelines are hereby adopted pertaining to the review of applications and recommendations to the City Council to fill vacancies on the Planning Commission:

I. City Council Ad -Hoc Subcommittee

1. The Mayor shall appoint an ad -hoc subcommittee at a regularly scheduled City Council meeting, and said committee shall consist of two (2) Councilmembers, with approval of a majority of Councilmembers present.

2. The notice of vacancy shall be posted by the City Clerk in accordance with State law.

3. The ad -hoc subcommittee shall review all complete applications that are received prior to the published date and time deadline for a commission vacancy. Applicants may not submit additional information after the filing deadline, nor may members of the ad- hoc subcommittee or City staff request additional information or materials after the filing deadline.

4. The ad- hoc subcommittee shall report its findings and recommendations to the City Council in a regular public City Council meeting. Consensus by the ad- hoc subcommittee is not required for consideration of an applicant by the full City Council.

5. The ad -hoc subcommittee shall be automatically disbanded (without further action required by the City Council) upon the appointment(s) of new Commissioner(s) and all vacancies on the Planning Commission have been filled.

II. Criteria for Review of Applications

1. Eligible applicants shall be residents of the City of Redlands and registered to vote at the time of filing the application. Councilmembers may consider the applicant's length of residency as well as knowledge of local planning or community development trends and issues.

2. Councilmembers shall consider the applicant's background, training, and/or professional experience and its relevance to the Planning Commission's duties and responsibilities. Preference will be given to applicants who have knowledge, training, and/or experience that are directly related to and will contribute meaningfully to the Planning Commission's responsibilities. Relevant fields of knowledge, training, or experience include, but are not limited to, urban planning, architecture, civil engineering, landscape architecture, real estate, real estate development, community development, economic development, environmental policy, public policy, public administration, finance and business administration.

3. Councilmembers may also consider other relevant factors such as: the applicant's demonstrated history of civic involvement in Redlands; previous positions and performance on other City of Redlands boards, commissions, or committees; or other volunteer or civic experience, and its relevance to the Planning Commission's duties and responsibilities.

4. Special consideration should be given to achieving a variety or diversity of backgrounds and representation on the Planning Commission, as this will contribute to a more fully informed analysis and public deliberation of topics by the entire Planning Commission.

5. Ad hoc subcommittee members mayshall personally interview all finalists prior to making its recommendation(s) to the City Council.

III. Planning Commissioner Training

1. Planning Commnnnissioners must maintain compliance with certain public official training requirements, including completing training courses for ethics and sexual harassment prevention.

2. The Development Services Department will provide introductory~~01y~~ training for new Commissioners as soon as practicable after appointment.

3. The Development Services Department will provide relevant training for all Commissioners on an annual or as-needed basis. Commissioners may obtain training from external providers or conferences, with registration costs (including costs for any books or related course materials) paid by the City, subject to budget availability and pre-authorization by the Development Services Director.

Section 2. California Environmental Quality Act. The proposed Resolution does not require environmental review in accordance with Sections 1506l(b)(3) and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 1 5378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the adoption of the Resolution may have a significant effect on the environment, insofar as it would establish administrative procedures and guidelines for reviewing applications to fill vacancies on the City of Redlands Planning Commission.

Section 3. Resolution No. 8674 is hereby rescinded.

Section 4. Effective Date. This Resolution shall take effect upon adoption. ~~of Ordinance No. 2981.~~

ADOPTED, SIGNED AND APPROVED this 6th~~15th~~ day of October~~April~~, 202~~65~~.

Mario Saucedo, Mayor

ATTEST:

Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk of the City of Redlands, do hereby certify that the foregoing Resolution was duly adopted by the City Council at a regular meeting thereof held on the 6th~~15th~~ day of October~~April~~, 2026~~5~~, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. J4.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Discussion and possible action relating to the formation of, and appointments to, an Ad Hoc Committee of the City Council to review applications for vacancies of the Planning Commission (Mayor Saucedo)

MOTION:

If the City Council concurs with Mayor Saucedo's recommendation, the following motions are provided:

1. I move to approve the formation of an Ad Hoc Committee of the City Council to review all applications from the Planning Commission candidates.

2. I further move to appoint _____ and _____ to the Ad Hoc Committee.

RECOMMENDATION:

It is recommended by Mayor Saucedo that the City Council form an Ad Hoc Committee of the City Council to review all applications for the Planning Commission and appoint two Council members to the committee.

DISCUSSION:

The process for filling a vacancy on the Planning Commission requires the Mayor to appoint an ad-hoc committee at a regularly scheduled City Council meeting, and said committee shall consist of two (2) Council members, with approval of a majority of Council members present. The ad hoc committee shall review all complete applications that are received prior to the published date and time deadline for a commission vacancy. Applicants may not submit additional information after the filing deadline, nor may members of the ad hoc committee or City staff request additional information or materials after the filing deadline. Furthermore, the ad hoc committee shall report its findings and recommendations to the City Council in a regular public City Council meeting. Consensus by the ad hoc committee is not required for consideration of an applicant by the full City Council. The ad hoc committee will not be subject to the Brown Act as it will be limited in scope and duration.

Once the City Council reviews the work of the committee and the matter is finalized, the ad hoc committee will automatically dissolve.

SUBMITTED BY:
Mayor Saucedo

REVIEWED BY:
Charles M. Duggan Jr., City Manager
Yvette M. Abich Garcia, City Attorney

PREPARED BY:
Whitney Mesna, Management Analyst

FISCAL IMPACT

Fiscal Year: 2026-27

Revenue Generating: No

Amount: N/A

Budgeted Y/N:

Account No.:

Additional Appropriation Required: Yes or No

Discussion:

There is no fiscal impact associated.

City Council **AGENDA ITEM NO. K1.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: CONTINUED PUBLIC HEARING to consider Ordinance Text Amendment No. 372 to amend Title 18 (Zoning Regulations) of the Redlands Municipal Code to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses; consideration of a proposed amendment to Chapter 18.156, Article XII (Warehouses and Logistics Distribution Centers) to add new Section 18.156.970 for new rebuilding provisions for existing warehouses and logistics distribution centers; and consideration of Resolution No. 8793 to amend the commercial and industrial Specific Plans of the City of Redlands to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses. The proposal qualifies for exemption from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines (Development Services Director Reilly)

PROCEDURE FOR PUBLIC HEARING:

1. Mayor declares the meeting open as a public hearing.
2. Mayor calls upon Department Director for report.
3. Mayor calls for questions/comments from members of the City Council.
4. Mayor calls for comments/questions/testimony from members of the public (3 minutes per speaker)
5. Mayor calls upon City Clerk to note any written comments received.
6. Mayor closes the public hearing.
7. City Council considers the motion and votes.

MOTION:

If the City Council determines that the Planning Commission's recommendation is appropriate, the following motions are provided:

1. I move to introduce Ordinance No. 3002 and find that the proposal is exempt from environmental review pursuant to Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines; and

2. I move to approve Resolution No. 8793 and find that the proposal is exempt from environmental review pursuant to Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines.

RECOMMENDATION:

On May 12, 2026, the Planning Commission adopted Resolution No. 1745 and recommended approval of the ordinance (see City Council staff report of September 1, 2026, for additional background information).

Staff recommends that the City Council introduce Ordinance No. 3002, as revised, to include the changes to the Planning Commission recommendation that were requested by Council on September 1, 2026, and approve Resolution No. 8793.

BACKGROUND:

On September 1, 2026, the City Council considered the proposed amendment and received public comments (Attachment A – City Council Staff Report). Council members discussed matters such as the maximum building height currently allowable in commercial and industrial zoning districts, potentially allowing modifications for warehouses to increase building height up to the maximum that is generally allowable within an applicable zone, and that any proposal to increase building height should be required to demonstrate that there will be a net environmental benefit (such as improved energy efficiency). The Council provided direction to staff to add language to the draft ordinance.

DISCUSSION:

Existing Warehouse Ordinance: The City's existing warehouse ordinance currently includes language that requires improvements and energy efficiencies to be incorporated into redevelopment projects to the extent feasible. The existing warehouse development standards contained in RMC Chapter 18.156, Article XII (see Attachment B) include categories for: sustainable energy; screening and buffering; traffic patterns and signs; and operation and construction. The requirements for sustainable energy state that: new warehouses must have "cool roof" materials; at least 90% of the on-site motorized equipment must be Zero Emission; and electricity supply must be from a photovoltaic (PV) solar collector system or other renewable energy source, to the extent feasible, while allowing for electricity demand that exceeds the generation capacity of the on-site renewable energy system to be obtained from off-site energy sources or suppliers. The existing zoning code provisions recognize that there may be constraints or limitations to generating and/or storing 100% of the energy needed on-site (such as the cost and space for providing large batteries on-site, Building Code and Fire Code requirements for lithium-ion batteries, construction and separation requirements, a Building Code requirement that the cost of installing solar PV systems be recouped by the developer within 15 years, and so on). The Planning Commission would ultimately decide the matter of feasibility, and it would be the applicant's responsibility to justify and explain why a particular element would not be feasible or possible for their project.

California Building Code: For most voluntary property redevelopment scenarios that involve raising existing roof height, the existing building would most likely need to be completely demolished and then reconstructed from the ground up. All-new construction would need to comply with the current Title 24 requirements of the California Building Code which includes the newest requirements for energy efficiency. The current California Building Code is far more stringent in terms of reducing energy demand and electricity use when compared to previous versions of the Building Code from prior years, and the normal course of reviewing building permit applications would require changing light fixtures to LEDs, installation of photovoltaic (PV) solar systems, cool roof materials, installation of electric vehicle (EV) charging systems, etc. Many of these provisions of the Building Code align with the goals and provisions of the City's current warehouse ordinance.

California Building Codes have become substantially more stringent over previous code cycles, and the 2025 Building Code has improved the nonresidential building efficiency by at least 33.5% over the 2013 standards. In other words, completely reconstructing a warehouse building under current or future Building Codes would be expected to result in a new structure that is a minimum of 33.5% more efficient in terms of energy use, simply by being constructed in accordance with current Building Codes. Requirements of the City's zoning regulations, such as those pertaining to site improvements and operations (e.g., installing EV charging systems for vehicles and trailer refrigeration systems, as well as requiring at least 90% of the on-site motorized equipment to be Zero Emission) would be expected to further reduce greenhouse gas emissions and environmental effects. Additional requirements in the City's zoning regulations pertaining to on-site improvements (such as landscape screening/buffering from adjacent land uses, truck routing provisions, prohibiting truck parking and queuing on public streets, cool surfaces within parking areas and drive aisles, etc.) further reduce environmental effects.

Changes to Draft Ordinance: Following the discussion by Council on September 1, 2026, the following changes have been made to the proposed draft ordinance:

1) The provision limiting any increase in building height to 15% above the existing height has been changed to allow for an increase up to the maximum building height that is generally applicable within the zone. In most cases, the maximum building height is limited to 50 feet (e.g., M-1, M-2, M-P zones as well as the EV/IC and EV/IR districts). Additional language is included to state that the maximum shall be 50 feet for warehouses if the zoning development standards do not specify a maximum building height (e.g., the C-M and I-P zones).

2) Proposed new Section 18.156.970(C) has been updated to include a provision requiring an applicant to prepare and submit an energy audit analysis in conjunction with a development application (e.g., Conditional Use Permit). In addition to the energy analysis that is already required during the Plan Check process for building permits (Title 24 compliance for new construction), this added provision would require an energy audit report for the existing facility to establish the baseline of its current energy demand, and then both analyses would need to be submitted with the development application for purposes of review by the Planning Commission. This would quantify the existing and proposed energy use and related efficiencies. It is expected that the reconstructed facility will improve (reduce) its energy consumption and reduce the stationary source environmental effects (e.g., greenhouse gases, air quality, etc.).

Furthermore, the provisions of the City's existing warehouse development standards would also continue to be applicable (such as requiring on-site energy generation systems, electric vehicle (EV) connections and charging systems, cool roof treatments, cool surface treatments and shading within parking lots, truck traffic controls and signage, screening and buffering from abutting land uses, on-site operational standards, etc.). As described previously, the feasible provisions of the City's existing warehouse ordinance (RMC Chapter 18.156 Article XII) would be imposed through the Conditional Use Permit process, subject to review and approval by the Planning Commission.

ENVIRONMENTAL REVIEW:

The proposed code amendment is exempt from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore is not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the zoning code amendment and specific plan amendment(s) may have a significant effect on the environment. Furthermore, even if the proposal is considered a project, the proposed zoning code amendment and specific plan amendment(s) are categorically exempt under CEQA Guidelines Section 15308, because it is clear that they will not create an environmental impact and the action will assure the maintenance, enhancement, or protection of the environment through the adoption of regulations and development standards on such warehouse and distribution facilities. Accordingly, no further environmental review is necessary.

ALTERNATIVES:

The City Council may consider these alternatives:

A. Modify the proposed ordinance language to include or exclude other provisions.
B. Provide additional direction to staff, and request that staff bring back a revised ordinance and resolution to a future City Council meeting.
C. Request additional information.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Sean Reilly, Development Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Brian Foote, City Planner

FISCAL IMPACT

Fiscal Year:

Revenue Generating: N/A

Amount: N/A

Budgeted Y/N:

Account No.: N/A

Additional Appropriation Required:

Discussion:

N/A

Attachments

A_City_Council_staff_report_9012026.pdf
B_RMC_Chapter_18156_Article_XII.pdf
C-1_Ord_3002_Warehouses_legislative.pdf
C-2_Ord_3002_Warehouses_clean.pdf
D_Resolution_No_8793_Warehouses.pdf

City Council **AGENDA ITEM NO. K1.**

DATE: September 1, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: CONTINUED PUBLIC HEARING to consider Ordinance Text Amendment No. 372 to amend Title 18 (Zoning Regulations) of the Redlands Municipal Code to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses; consideration of a proposed amendment to Chapter 18.156, Article XII (Warehouses and Logistics Distribution Centers) to add new Section 18.156.970 for new rebuilding provisions for existing warehouses and logistics distribution centers; and consideration of Resolution No. 8793 to amend the commercial and industrial Specific Plans of the City of Redlands to prohibit new warehouses and logistics distribution facilities, as defined, and allow existing warehouses to remain as permitted or conditionally permitted uses. The proposal qualifies for exemption from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines (Development Services Director Reilly)

PROCEDURE FOR PUBLIC HEARING:

1. Mayor declares the meeting open as a public hearing.
2. Mayor calls upon Department Director for report.
3. Mayor calls for questions/comments from members of the City Council.
4. Mayor calls for comments/questions/testimony from members of the public (3 minutes per speaker)
5. Mayor calls upon City Clerk to note any written comments received.
6. Mayor closes the public hearing.
7. City Council considers the motion and votes.

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move to introduce Ordinance No. 3002 and find that the proposal is exempt from environmental review pursuant to Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines; and

2. I move to approve Resolution No. 8793 and find that the proposal is exempt from environmental review pursuant to Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines.

RECOMMENDATION:

On April 14, 2026, the Planning Commission discussed the draft ordinance language and made suggestions for changes including: add definitions for the terms *Alteration* and *Repair*; add additional language to reiterate that a property with a valid unexpired land use entitlement from the City (for a facility that has not yet been constructed) has the same land use rights as existing warehouses; and add provisions that would allow for an existing warehouse to increase the building height up to 15 percent and/or add more truck docking positions to the building, subject to approval of a Conditional Use Permit and certain additional criteria specified in the proposed code amendment (discussed further below).

On May 12, 2026, the Planning Commission reviewed the revised ordinance language, and adopted a resolution recommending that the City Council approve Ordinance Text Amendment No. 372 and the related Specific Plan Amendments.

On June 16, 2026, the City Council held a public hearing, received the staff presentation and public comments, and continued the public hearing (without any discussion or deliberation) to the September 1, 2026, regular City Council meeting.

BACKGROUND:

On October 14, 2025, the Planning Commission made a recommendation to the City Council to consider a code amendment to the Zoning Regulations (RMC Title 18) to prohibit any new warehouses or logistics distribution facilities from being established within the City.

On November 18, 2025, the City Council received public comments and provided direction to staff for a new ordinance. Council members discussed their intent to allow existing warehouses to remain as permitted uses, and if a warehouse were to be rebuilt (e.g., due to fire or other natural disaster), then it should only be reconstructed to the previously existing size (square-footage and height). Also, developers should not assemble properties for the purpose of redevelopment with a new large warehouse or expanding an existing warehouse.

Zoning Regulations (RMC Title 18): The City's current zoning regulations applicable to warehouses are contained in RMC Chapter 18.156, Article XII, titled Warehouses and Logistics Distribution Centers. The section includes the following definition of a "Warehouse" for purposes of the City's zoning regulations, which states such facilities are 50,000 square-feet or more in gross floor area or contain six (6) or more truck docks or dock high loading doors. Additional development standards also apply to the construction of new warehouses, including sections for screening/buffering, traffic patterns/signs, sustainable energy, operation, and site location.

Table 1. Warehouse definitions in the City of Redlands zoning regulations (RMC Title 18).

Warehouse:	Warehouse/distribution facilities primarily used for the storage and/or consolidation of manufactured goods before their distribution to retail locations or other warehouses. Warehouse/distribution centers are fifty thousand (50,000) square-feet or more in gross floor area or contain six (6) or more truck docks or dock high loading doors. They are characterized by dock high loading doors and could be on opposing sides of the building (cross dock facility); may include grade-level loading doors; interior clear heights a minimum of 28 to 36 feet to ceiling for the warehousing floor area; significant movement and storage of products, materials, or equipment; may include receiving, sorting, re-packaging, and/or re-distribution; truck activities frequently outside of the peak hour of the adjacent street system; and need freeway access. This definition excludes facilities owned and operated by a government agency or any public or private utilities. Warehousing and distribution facilities include, but are not limited to, the following types of uses: A. Warehousing distribution/high cube distribution centers. B. Parcel delivery terminals or truck terminals. C. Parcel sorting and distribution facilities. D. Package allocation for delivery drivers or independent delivery contractors. E. Parcel hub or high cube fulfillment center. F. Freight yards or forwarding terminals. G. Moving agencies. H. Shipping/receiving yards.
Warehousing, Ancillary:	The use of a portion of a building for the related storage of goods of any type by one or two businesses and used for the sale or distribution of those goods directly to their customers. A manufacturing, assembly, service commercial, or other type of commercial or industrial use (i.e., primary use) manufactures and/or stores and distributes the goods or components that are produced or contained on-site, and therefore includes the related storage of those goods or items. Ancillary storage or warehousing is subordinate and incidental to the primary land use (e.g., manufacturing, assembly, service commercial, or other type of primary commercial or industrial use). Ancillary storage or warehousing may include ground level loading doors on one or more sides of the building, or not more than five (5) dock high loading doors on one side of the building only.

Existing Zoning Districts for Warehousing: Currently, the Zoning Regulations (RMC Title 18) require approval of a Conditional Use Permit to construct or establish a new warehouse in the Commercial Manufacturing (C-M), Light Industrial (M-1), General Industrial (M-2), and Industrial (I-P) zones. In addition, several Specific Plans allow warehousing and distribution center uses, primarily on the westerly side of the City and within the East Valley Corridor Specific Plan area.

DISCUSSION:

A) Zoning Code Amendment

The proposed amendment to RMC Title 18 would prohibit any new warehouses in the following commercial and industrial districts: Commercial Manufacturing (C-M), Light Industrial (M-1), General Industrial (M-2), and Industrial (I-P) zones. Warehouse uses would be deleted from the Conditional Use lists for the C-M, M-1, M-2, and I-P zones.

The proposed amendment would allow existing warehouses to remain as Permitted or Conditionally Permitted uses by adding the following text to the respective use lists for each zone (note the M-2 zone incorporates by reference the Permitted uses of the M-1 zone).

Proposed text for the Permitted Uses sections would be:

> “Warehouses or logistics distribution centers, existing (as of the effective date of Ordinance No. 3002) with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.”

Proposed text for the Conditional Uses section (in the I-P, Industrial zone only):

> “Warehouses or logistics distribution centers, existing (as of the effective date of Ordinance No. 3002) with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid conditional use permit approved prior to the effective date of Ordinance No. 3002). Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.”

The following paragraph is proposed to be added to the Site Location Requirement (RMC Section 18.156.920) to prevent the assemblage of parcels for the purpose of expanding an existing warehouse or logistics distribution use (as suggested by Council).

> “B. Assemblage of Parcels Prohibited: No warehouse development project or redevelopment or reconstruction of a property for warehouse use, may assemble or merge additional properties for the purpose of developing, enlarging, expanding, or intensifying the use of an existing warehouse or logistics distribution facility.”

Furthermore, the Planning Commission recommended adding the following paragraph to the ‘Applicability’ section (RMC Section 18.156.910) to address situations where a property possesses a valid unexpired land use entitlement, but a warehouse facility has not yet been physically constructed as of the effective date of the ordinance.

> “C. A property with a valid unexpired land use entitlement for a new warehouse or logistics distribution facility that has not yet been constructed or established as of the effective date of Ordinance No. 3002 shall have the same land use rights as if the structure had been existing on the effective date of Ordinance No. 3002.”

Provisions for Rebuilding

As existing warehouses would be allowed to remain as Permitted or Conditionally Permitted uses, the usual nonconforming provisions of the zoning regulations contained in RMC Chapter 18.184 (Nonconforming Buildings and Uses) would not normally be applicable. Therefore, new provisions need to be created within RMC Chapter 18.156, Article XII (titled “Warehouses and Logistics Distribution Centers”) to allow existing warehouses to be fully rebuilt, repaired, renovated, etc., up to 100 percent of the previously existing gross floor area and previously existing building height. A new section is proposed, which would be Section 18.156.970, as follows:

> “18.156.970: REBUILDING PROVISIONS FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION CENTERS:
>
> A. Existing warehouses and logistics distribution facilities (as of the effective date of Ordinance No. 3002) may be rebuilt only to the previously existing square-footage and previously existing height if the structure meets the following criteria:
>
> 1. The warehouse or logistics distribution use was legally established prior to the effective date of Ordinance No. 3002; or if not yet established, the subject property had a valid land use entitlement issued prior to the effective date of Ordinance No. 3002.
>
> 2. The Development Services Director has determined the existing business to be a permitted or conditionally permitted use.
>
> 3. A change in ownership or tenancy without any change in use or occupancy shall not affect any of the rebuilding rights, privileges, and responsibilities provided pursuant to this section.

4. It shall be the property owner's responsibility to provide evidence or information to justify the establishment of rebuilding rights.

B. Criteria for rebuilding, reconstruction, renovation, or improvements to an applicable structure or property.

1. Ordinary repair and maintenance may be performed on a structure or property subject to these provisions, in accordance with applicable law (e.g., California Building Code, California Fire Code, etc.).

2. Improvements to the existing structure including technology upgrades (e.g., seismic strengthening, energy use efficiency, PV solar or re-roof, water use efficiency, reductions to greenhouse gas emissions, hazardous materials remediation, etc.) may be installed on a structure or property subject to these provisions, in accordance with applicable law.

3. Warehouses and logistics distribution facility buildings may be voluntarily rebuilt, reconstructed, renovated or refurbished if the permitted square-footage (gross floor area) is not increased and building height is not increased, and subject to the provisions of this article.

4. If involuntarily damaged or destroyed by a catastrophic event (fire, flood, earthquake or other calamity, by act of God or by the public enemy), the entirety of the structure may be rebuilt to the previously existing permitted square-footage (gross floor area) and previously existing height."

Provisions for Increasing Building Height

The Commission also recommended adding provisions to the proposed Section 18.156.970 that would allow for an increase to building height and/or truck dock positions, if the property owner applies for a Conditional Use Permit and includes any feasible provisions of RMC Chapter 18.156, Article XII (e.g., sustainable energy features, screening/buffering improvements, traffic patterns/signage requirements, and operational requirements). The additional criteria would be the following.

"C. Existing warehouses and logistics distribution facilities (existing as of the effective date of Ordinance No. 3002) may be altered and request an increase to the building height pursuant to the following criteria:

1. Building height may be increased up to 15% over the existing roof height (and overall building height not to exceed the maximum height allowable within the applicable land use district) to incorporate technology upgrades, energy efficiency improvements, or other justifiable economic or environmental reasons; and/or may increase the number of previously existing truck dock positions; provided the structure meets the criteria listed below.

a. The subject property meets all applicable criteria in Section 18.156.970(B).

b. The subject property obtains a Conditional Use Permit issued pursuant to Chapter 18.192 of this title.

c. Construction or redevelopment of a building involving additional height shall include the feasible provisions of Section 18.156.930 through 18.156.960 of this article, as determined by the Planning Commission (the location requirements of Section 18.156.920(A) shall not apply). For purposes of this article, "feasible" has the same meaning as California Code of Regulations Title 14, § 15364.

d. Complete an environmental review process, if applicable, in accordance with the California Environmental Quality Act for a proposed project that will increase building height, increase the number of truck docks, or change non-refrigerated space to refrigerated space.

e. The commission may require one or more of the following in instances where the proposed redevelopment, reconstruction, or alteration appears to create impacts to traffic, landscaping, or economic feasibility:

i. Circulation studies, prepared by a traffic engineer, showing the movement of vehicular and truck traffic to and from the subject property, and to and from existing thoroughfares. Special engineering features and/or traffic regulation devices needed to facilitate or ensure safety of circulation may be required;

ii. A landscaping and tree planting plan, prepared by a landscape architect;

iii. An economic feasibility report or market analysis, prepared by a qualified economist, justifying the need to increase the building height and/or increase the number of truck docks."

The Commission discussed and recommended adding the phrase "or an applicable entitlement " to element (C)(1) above regarding maximum allowable height ("...and overall building height not to exceed the maximum height allowable within the applicable land use district or an applicable entitlement"). However, the provision for "an applicable entitlement" may be inconsistent with their intent to allow for a 15% increase to existing building height, as most development projects are already constructed to the height specified in their entitlements (such as a Commission Review & Approval permit, Conditional Use Permit, or Planned Development entitlement). In terms of practical effects, limiting the height to "an applicable entitlement" may not allow for any height increase whatsoever in some circumstances. The typical maximum allowable building height is 50 feet in the M-1, M-2, EV/IC and EV/IR districts (and none specified in the C-M and I-P districts). However, limiting maximum height to that stated in an approved entitlement (such as 40 feet or 44 feet, for example) would be more restrictive than the 50-foot maximum that is generally applicable to other properties located within the same zoning district, in most cases. Council may wish to remove the language making reference to "an applicable entitlement" for internal consistency. Lastly, "interior ceiling height" should be changed to "building height" for consistency (see Attachment A-1, Draft Ordinance, legislative version illustrating the changes).

Definitions for Alteration and Repair

The Commission recommended adding definitions for the terms *Alteration* and *Repair*, which would largely mirror the existing definitions as contained in the California Building Code. The Commission recommended adding the word "interior" to the definition of *Alteration* so that it only refers to interior building modifications, not to other exterior site improvements or maintenance activities that do not affect the building.

Proposed definition of *Alteration* (based on California Building Code definition).

> Any construction or renovation to an existing structure other than repair or addition. A change, addition or modification in construction, change in occupancy or use, or structural repair to an existing building or facility. Alterations include, but are not limited to, remodeling, renovation, rehabilitation, reconstruction, historic restoration, resurfacing of interior circulation paths or vehicular ways, changes or rearrangement of the structural parts or elements, and changes or rearrangement in the plan configuration of walls and full-height partitions. Normal maintenance, reroofing, painting or wallpapering, or changes to mechanical and electrical systems are not alterations unless they affect the usability of the building or facility.

B) Specific Plan Amendments

Similar amendments to the use lists of commercial and industrial Specific Plans will adopt similar provisions as well as refer to RMC Title 18. These include the following:

- East Valley Corridor Specific Plan (Specific Plan No. 40);
- East Valley Complex (Specific Plan No. 25);
- Redlands Aviation Park (Specific Plan No. 32);
- Centennial Commerce Park (Specific Plan No. 33);
- Redlands Research Park (Specific Plan No. 42);
- Concept Plans (CP-1 and CP-2); and,
- Planned Developments (PD Nos. 1, 3, 4, and 7) within the East Valley Corridor Specific Plan.

C) Environmental Review

The proposed code amendment is exempt from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the zoning code amendment and specific plan amendment(s) may have a significant effect on the environment. Furthermore, even if the proposal is considered a project, the proposed zoning code amendment and specific plan amendment(s) are categorically exempt under CEQA Guidelines Section 15308, because it is clear that they will not create an environmental impact and the action will assure the maintenance, enhancement, or protection of the environment through the adoption of regulations and development standards on such warehouse and distribution facilities. Accordingly, no further environmental review is necessary.

ALTERNATIVES:

The City Council may consider these alternatives:

A. If Council does not wish to allow for an increase to existing building height and/or additional truck docks, Council may modify the proposed ordinance to exclude the relevant provisions (delete proposed section 18.156.970(C) pertaining to building height increase, or delete portions referencing additional truck docks).
B. Council may modify the proposed ordinance language to include or exclude other provisions.
C. Provide additional direction to staff, and request that staff bring back a revised ordinance and resolution to a future City Council meeting.
D. Request additional information.

SUBMITTED BY:
Sean Reilly, Development Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Kurt Wilson, Assistant City Manager
Danielle Garcia, Assistant City Manager
James Garland, Interim Finance Director

PREPARED BY:
Brian Foote, City Planner

Attachments

B-1_Resolution_No_8793_-_Warehouses.pdf
A-1_Ord_3002_Warehouses_legislative.pdf
A-2_Ord_3002_Warehouses_clean.pdf

ARTICLE XII. WAREHOUSES AND LOGISTICS DISTRIBUTION CENTERS

18.156.900: DEFINITIONS:

WAREHOUSE:	Warehouse/distribution facilities primarily used for the storage and/or consolidation of manufactured goods before their distribution to retail locations or other warehouses. Warehouse/distribution centers are fifty thousand (50,000) square-feet or more in gross floor area or contain six (6) or more truck docks or dock high loading doors. They are characterized by dock high loading doors and could be on opposing sides of the building (cross dock facility); may include grade-level loading doors; interior clear heights a minimum of 28 to 36 feet to ceiling for the warehousing floor area; significant movement and storage of products, materials, or equipment; may include receiving, sorting, re-packaging, and/or re-distribution; truck activities frequently outside of the peak hour of the adjacent street system; and need freeway access. This definition excludes facilities owned and operated by a government agency or any public or private utilities. Warehousing and distribution facilities include, but are not limited to, the following types of uses: A. Warehousing distribution/high cube distribution centers. B. Parcel delivery terminals or truck terminals. C. Parcel sorting and distribution facilities. D. Package allocation for delivery drivers or independent delivery contractors. E. Parcel hub or high cube fulfillment center. F. Freight yards or forwarding terminals. G. Moving agencies. H. Shipping/receiving yards.
WAREHOUSING, ANCILLARY:	The use of a portion of a building for the related storage of goods of any type by one or two businesses and used for the sale or distribution of those goods directly to their customers. A manufacturing, assembly, service commercial, or other type of commercial or industrial use (i.e., primary use) manufactures and/or stores and distributes the goods or components that are produced or contained on-site, and therefore includes the related storage of those goods or items. Ancillary storage or warehousing is subordinate and incidental to the primary land use (e.g., manufacturing, assembly, service commercial, or other type of primary commercial or industrial use). Ancillary storage or warehousing may include ground level loading doors on one or more sides of the building, or not more than five (5) dock high loading doors on one side of the building only. (Ord. 2955, 2023)

18.156.910: APPLICABILITY:

The provisions of this section shall apply to the following types of development projects:

A. New warehouse development projects that meet one of the following criteria (note: excludes government agency facilities and public or private utility facilities).

1. Gross floor area of fifty thousand (50,000) square-feet or more; or,

2. A structure with six (6) or more truck docks or dock high loading doors (does not include grade-level loading doors or loading spaces).

B. Development or redevelopment projects for existing or proposed warehouse facilities involving demolition, reconstruction, repairing, or rebuilding that exceed fifty percent (50%) of the reasonable replacement value of the existing structure or property.

1. Estimates for this purpose shall be reviewed and approved by the building official and the Development Services Director, or their respective designees, and shall be based on the minimum cost of construction in compliance with the California Building Code.

2. For the purpose of this section, "assessed value" shall mean the assessed value of the structure as shown on the County of San Bernardino property assessment roll in effect at the time of the occurrence of the casualty, or at the time the repair and maintenance is first conducted.

3. Redevelopment of a property and/or building shall include the feasible provisions of Section 18.156.930 through 18.156.960 of this Article, as determined by the Planning Commission.

C. Required Compliance. No new warehouse development project shall be constructed, no redevelopment or reconstruction of a property for warehouse use, and no existing warehouse shall be moved, altered, or enlarged, except in accordance with the applicable development standards of this Article. (Ord. 2955, 2023)

18.156.920: SITE LOCATION REQUIREMENT:

No warehouses shall be located on a project site more than one mile (5,280 feet) from a freeway entrance/exit ramp to the Interstate Freeway System (Interstate 10 and Interstate 210). For purposes of this requirement, the linear distance shall be measured as a radius from a freeway ramp to any part of the subject property. (Ord. 2955, 2023)

18.156.930: SCREENING AND BUFFERING REQUIREMENTS:

A. Warehouse developments shall provide a solid decorative wall(s) of at least ten feet (10') in height when abutting any sensitive receptors. Sensitive receptors for purposes of this section shall be defined as any residence including private homes, condominiums, apartments, and living quarters, schools, preschools, daycare centers, in-home daycares, hospitals, long-term care facilities, retirement and nursing homes, community centers, places of worship, parks (excluding trails), and dormitories. The exterior treatment of the wall(s) shall be decorative or painted.

B. Unless physically impossible, loading docks and truck entries shall be oriented away from abutting sensitive receptors. To the greatest extent feasible, loading docks, truck entries, and truck drive aisles shall be located away from nearby sensitive receptors. In making feasibility decisions, the City must comply with existing laws and regulations and balance public safety and the site development's potential impacts to nearby sensitive receptors. Therefore, loading docks, truck entries, and drive aisles may be located nearby sensitive receptors at the discretion of the Planning Commission, but any such site design shall include measures designed to minimize overall impacts to nearby sensitive receptors.

C. Trees shall be used as part of the solid screen buffering treatment for any adjacent residential properties or properties with sensitive receptors. Trees used for this purpose shall be evergreen, drought-tolerant, minimum 36-inch box size, and shall be spaced no greater than forty (40)-feet on center. Palm trees shall not be used for screening purposes. The property owner and any successors in interest shall maintain these trees for the duration of ownership ensuring any unhealthy or dead trees are replaced timely as needed.

D. Trees shall be installed in automobile (passenger vehicle) parking areas to provide at least thirty five percent (35%) shade cover of parking areas within fifteen (15) years. This requirement is in addition to the applicable standard design requirements for parking lot landscape and related improvements. Trees shall be planted that are capable of implementing this requirement. (Ord. 2955, 2023)

18.156.940: TRAFFIC PATTERNS AND SIGN REQUIREMENTS:

A. Applicants for entitlements shall prepare and submit a Truck Routing Plan demonstrating the most direct route(s) to and from the Interstate Freeway System based on the city's latest Truck Route Map. Routes to or from freeway ramps shall not pass through any residential zones or districts.

B. A traffic impact assessment (TIA) report shall be prepared to evaluate a proposed warehouse project's compliance with the City's Measure U traffic system requirements, and shall include an evaluation of the City's streets and Truck Routes that provide vehicular access to the Interstate Freeway System, including, but not limited to: existing right-of-way width; roadway capacity to handle the proposed quantity of truck trips to be generated by the proposed use (including any road widening that may be necessary); roadway design and improvements to handle the weight and frequency of proposed truck trips; intersection operations to freeway ramps and level of service analysis to include the proposed truck trips; truck turn radii at intersections; and other operational elements of the City's street network to serve the proposed use. The TIA may be prepared by a qualified consultant selected and directed by the City (and all consultant costs to be reimbursed by the applicant), or by a qualified traffic consultant selected by the applicant (and all work subject to the direction, review, and approval by the City).

C. Entry gates into the loading dock/truck court area with more than twenty (20) loading docks shall be positioned after a minimum of one hundred forty (140) feet of total available stacking depth inside the property line (or alternatively, if one hundred forty (140) feet of depth is not feasible due to site constraints, then provide seventy (70) feet of available stacking depth for two trucks side-by-side as an alternative design). The stacking distance shall be increased by seventy (70) feet for every twenty (20) loading docks beyond 50 docks. Queuing, or circling of vehicles, on public streets immediately pre- or post-entry to an industrial commerce facility is strictly prohibited unless queuing occurs in a deceleration lane or right turn lane exclusively serving the facility.

D. Prior to entitlement approval, applicants shall submit to the City, and obtain approval of, all turning templates to verify adequate truck turning movements at entrance and exit driveways as well as street intersections adjacent to industrial buildings. Unless not physically possible, truck entries shall be located on Collector streets or streets of a higher commercial classification, and vehicle entries shall be designed to prevent truck access on streets that are not Collector Streets (or streets of a higher commercial classification), including but not limited to by limiting the width of vehicle entries.

E. Anti-idling signs indicating a five (5) minute restriction on engine idling for diesel trucks shall be posted at warehouses and industrial commerce facilities along entrances to the site and within the dock areas and shall be strictly enforced by the facility operator (13 CCR § 2480).

F. Signs shall be installed at all truck exit driveways directing truck drivers to the truck route as indicated in the Truck Routing Plan to be routed to the Interstate Freeway System.

G. Signs and drive aisle pavement markings shall clearly identify the onsite circulation pattern to minimize unnecessary on-site vehicular travel.

H. Facility operators shall post signs in prominent locations inside and outside of the building indicating that off-site parking for any Medium Heavy-Duty trucks, Heavy Heavy-Duty trucks, truck trailers or cabs, and other operations-related vehicles is strictly prohibited. City may require facility operator to post signs on adjacent and nearby surface or residential streets indicating that off-site truck parking is prohibited by City ordinance.

I. All signs under this Section shall be legible, durable, and weather-proof. (Ord. 2955, 2023)

18.156.950: SUSTAINABLE ENERGY:

A. A minimum of ninety percent (90%) of the on-site motorized operational equipment shall be zero emission (ZE).

B. All warehouse building roofs shall install photovoltaic (PV) solar collector system or other form of on-site renewable energy, provided such renewable energy source is recognized by the State of California as a renewable resource under the Renewable Portfolio Standard Program. The renewable energy system shall be metered separately from the nonrenewable metered power usage of the building (if not in conflict with other applicable regulations). The renewable energy system shall be built to generate an amount of electricity sufficient to meet the following criteria:

1. Annualized building demand based on the approved use or, if no use is proposed, then the demand for the most energy intensive use that could occupy the building; and

2. Annualized demand required to charge fully electric vehicles and trucks, assuming that all vehicles and trucks to the site are fully electric; and

3. A reasonable rate of efficiency loss over ten (10) years.

Note: Electricity demand that exceeds the generation capacity of the on-site renewable energy system may be obtained from off-site energy sources or suppliers.

C. The warehouse building's rooftop that is not covered with solar panels or other utilities shall be constructed with light colored roofing material with a solar reflective index (SRI) in accordance with current California Energy Code regulations. This material shall be the minimum solar reflective rating of the roof material for the life of the building.

D. The on-site passenger vehicle parking shall include electric vehicle (EV) ready parking spaces in accordance with current requirements of the California Building Code, and at least fifty percent (50%) of the required EV parking spaces shall be equipped with working Level 2 Quick Charge EV charging stations installed and operational, prior to building occupancy. Signage shall be installed indicating EV charging stations and specifying that spaces are reserved for clean air/EV vehicles. Unless superior technology is developed that would replace the EV charging units, facility operator and any successors in interest shall be responsible for maintaining the EV charging stations in working order for the life of the facility.

E. Unless the owner of the facility records a covenant on the title of the underlying property ensuring that the property cannot be used to provide chilled, cooled, or freezer warehouse space, a conduit shall be installed during construction of the building shell from the electrical room to all (100%) of the loading dock doors that have potential to serve the refrigerated space. When tenant improvement building permits are issued for any refrigerated warehouse space, electric plug-in units shall be installed at every dock door servicing the refrigerated space to allow transport refrigeration units (TRUs) to plug in. Truck operators with TRUs shall be required to utilize electric plug-in units when at loading docks. (Ord. 2955, 2023)

18.156.960: OPERATION AND CONSTRUCTION:

A. Cool surface treatments shall be added to all drive aisles and parking areas, or such areas shall be constructed with a solar-reflective cool pavement such as concrete. Solar collectors may be installed on support structures that provide shade over parking areas to achieve minimum requirements.

B. To ensure that warehouse electrical rooms are sufficiently sized to accommodate the potential need for additional electrical panels, either a secondary electrical room shall be provided in the building, or the primary electrical room shall be sized twenty-five percent (25%) larger than is required to satisfy the service requirements of the building or the electrical gear shall be installed with the initial construction with twenty-five percent (25%) excess demand capacity.

C. All exterior light fixtures (including but not limited to parking lot lighting, wall fixtures, roof fixtures, light poles, etc.) visible from public right-of-way or abutting properties shall have shielding affixed to contain illumination within the subject property and prevent light trespass and glare overspill.

D. The facility operator shall be required to perform regular maintenance of building structures, landscaping, and paved surfaces to ensure good physical condition and appearance.

E. For any sites with warehouses that are abutting or adjacent to any residential properties or properties containing sensitive receptors, any outdoor storage of materials, high-pile storage, or any other manner of storage or staging shall not exceed the height of the perimeter wall.

F. Additional operating conditions may be enacted for an individual Warehouse project pursuant to a Conditional Use Permit (RMC Chapter 18.192) for the purpose of avoiding or reducing potential off-site nuisance effects of the warehouse facility (including but not limited to traffic, parking, noise, vibration, air quality emissions, etc.) on nearby sensitive receptors or residential districts, or to protect the public health, safety, or general welfare. (Ord. 2955, 2023)

ORDINANCE NO. 3002

AN ORDINANCE OF THE CITY OF REDLANDS AMENDING TITLE 18 (ZONING REGULATIONS) OF THE REDLANDS MUNICIPAL CODE TO PROHIBIT NEW WAREHOUSING AND LOGISTICS DISTRIBUTION CENTERS, AS DEFINED, IN THE COMMERCIAL AND INDUSTRIAL ZONES, WHILE ALLOWING FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION USES TO REMAIN AS PERMITTED OR CONDITIONALLY PERMITTED USES SUBJECT TO NEW REBUILD PROVISIONS.

WHEREAS, the City Council of the City of Redlands has initiated Ordinance Text Amendment No. 372, in accordance with Chapter 18.204 (Amendments) of the Redlands Municipal Code, as the public necessity, convenience, or general welfare justifies such action; and

WHEREAS, over the past twenty years, Redlands has experienced the construction of numerous large warehouses and logistics distribution facilities in and around the City of Redlands including the unincorporated County jurisdiction located in northwest Redlands; and

WHEREAS, on September 29, 2024, the Governor of the State of California signed Assembly Bill (AB) 98 to add Section 65302.02 to, and to add Chapter 2.8 (commencing with Section 65098) to Division 1 of Title 7 of, the Government Code, and to add Sections 40458.5 and 40522.7 to the Health and Safety Code, relating to land use, and the "Warehouse Concentration Region" defined therein includes the City of Redlands among other nearby cities and counties; and

WHEREAS, two major transportation corridors (Interstate 10 and Interstate/S.R. 210 freeways) serve the Southern California region and are gateways to the Interstate Highway System, and both freeways pass through the City of Redlands, which contributes to a significant quantity of heavy-truck and other vehicular traffic to pass through the City to reach destinations located outside the City of Redlands as well as within the unincorporated "donut hole" area; and

WHEREAS, heavy-truck traffic that serves several million square feet of warehousing and logistics distribution uses located within the unincorporated County island area (surrounded by the City of Redlands) must pass through the City and utilize City streets on a daily basis at all hours of the day and night; and

WHEREAS, the residents and visitors of the City of Redlands may experience exposure to environmental effects (such as numbers of truck trips, vehicle miles traveled, greenhouse gas emissions affecting air quality, vehicular noise, etc.) and other externalities from such warehousing and logistics distribution uses; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about March 24, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on April 14, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about April 21, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on May 12, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, the proposed Ordinance No. 3002 is exempt from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines; and

WHEREAS, following the public hearing on May 12, 2026, the Planning Commission determined that Ordinance Text Amendment No. 372 would be in conformity with the 2035 General Plan, and would be consistent with goals of the General Plan for transportation, connectivity, compatibility and harmonious relationship of different land uses; and

WHEREAS, on May 12, 2026, the Planning Commission recommended approval of Ordinance Text Amendment No. 372 to the City Council; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, the City Clerk gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by City Council; and

WHEREAS, on June 16, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing; and

WHEREAS, on September 1, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing; and

WHEREAS, on September 1, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing to October 6, 2026; and

WHEREAS, on October 6, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF REDLANDS DOES ORDAIN AS FOLLOWS:

SECTION 1. California Environmental Quality Act. The proposed Ordinance Text Amendment does not require environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the zoning code amendment may have a significant effect on the environment, insofar as it would amend the lists of permitted land uses in the City of Redlands. Furthermore, even if the proposal is considered a project, the proposed zoning code amendment is categorically exempt under CEQA Guidelines Section 15308, because it is clear that it will not create an environmental impact and the action will assure the maintenance, enhancement, or protection of the environment through the adoption of regulations prohibiting new large new warehouses and logistics distribution facilities. Accordingly, no further environmental review is necessary.

SECTION 2. Redlands Municipal Code Section 18.100.040, entitled "Permitted Uses" for the Commercial Industrial (C-M) District, is hereby amended to read as follows:

"18.100.040: PERMITTED USES:

Principal permitted uses in the C-M zone include:

A. Auto services: No open service bays shall face a public street, or they shall be screened:

Brake relining.
Glass installation.
Muffler installation.
Painting.
Repair.
Upholstery.

B. Commercial sales and service:

Agricultural supplies and equipment.
Automobile equipment.
Automobile, new and used.
Bicycle, boat and motorcycle.
Building material and hardware.
Cabinet shop.
Camper and mobilehome.
Drive-in stores, such as milk and food, no alcohol beverage sales.
Electrical apparatus and equipment.
Furniture, appliances and carpeting.

Garden and farm supplies.
Interior decorator studios.
Machinery, equipment and supplies.
Nurseries; no outdoor display of merchandise other than plants.
Office equipment.
Paint.
Pet and pet supply.
Plumbing, heating, air conditioning and refrigeration equipment and supplies.
Radio, television and musical instruments.

C. Industrial:

Uses permitted in the M-P planned industrial district.

Recreation and entertainment: The following uses are subject to approval of a conditional use permit if within three hundred feet (300') of a residential area:

Bowling lanes, skating rinks, and sports arenas, no alcohol beverage sales.
Drive-in theaters.

D. Services:

Auction houses.
Auto rental.
Bus terminals and similar transit facilities.
Cleaning and dyeing plants, laundries, linen and towel service.
Furniture upholstery.
Governmental agencies.
Ice manufacture, cold storage, and frozen food lockers.
Mail order houses.
Motels and hotels.
Parcel delivery.
Pest control.
Public scales.
Radio and television broadcasting studios.
Restaurants.
Retreading of tires.
Sign painters.

E. Other uses:

Agricultural uses permitted in the M-P district.
Business, technical, trade or professional schools.
Clubs, lodges, and similar organizations.
Electric distribution substations, public utility buildings and service yards.
Van and storage.

Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).
Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.
Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.
Wholesalers."

SECTION 3. Redlands Municipal Code Section 18.100.070, entitled "Conditional Uses" for the Commercial Industrial (C-M) District, is hereby amended to read as follows:

"18.100.070: CONDITIONAL USES:

The following uses may be permitted in the C-M zone subject to approval of a conditional use permit:

Uses listed in chapter 18.192 of this title.
Ambulance service.
Animal hospitals.
Bowling lanes, skating rinks, and sports arenas, with alcohol beverage sales.
Cocktail lounges and bars.
Drive-in stores, such as milk and food, with alcohol beverage sales.
Equipment rental.
Radio and television transmitter towers higher than fifty feet (50') above ground level.
Regional shopping center containing at least one department store and a minimum gross land area of thirty five (35) acres; uses permitted shall be limited to those contained in the C-3 zone.
Retail store containing a minimum gross leasable area of seventy five thousand (75,000) square feet, subject to the parking requirements for neighborhood commercial districts.
Service stations.
~~Warehouses and logistics distribution centers, in accordance with chapter 18.156 of this title~~."

SECTION 4. Redlands Municipal Code Section 18.108.030, entitled "Permitted and Accessory Uses" for the (M-1) Light Industrial District is hereby amended to read as follows:

"In the M-1 zone, principal permitted uses shall be as follows:

A. Uses permitted in the M-P, planned industrial district.

B. Accessory uses:

Commercial sales and service incidental to a principal permitted use.
Employee recreational facilities and play areas.
Storage buildings incidental to a permitted use.
Superintendent or caretaker dwelling. One dwelling unit on the same parcel of land as a

permitted use needing continual supervision, to be occupied exclusively by a superintendent or a caretaker and his family.
Other accessory uses and buildings customarily appurtenant to a permitted use.

C. Manufacturing:

Manufacture and assembly of electrical equipment and supplies, such as coils, condensers, lamps, switches, wire and cable assembly.

Manufacture of ceramic products, such as pottery, figurines and small glazed tile, utilizing only previously pulverized clay, and provided that kilns are fired only by electricity or gas.

Manufacture of cutlery, hardware, hand tools and kitchen utensils.

Manufacture, processing or treatment of products other than those which may be obnoxious or offensive by reason of emission of odor, dust, smoke, gas, noise, vibration or hazard.

Manufacturing, assembling, compounding, packaging and processing of articles or products from the following previously prepared materials: asbestos, bristles, bone, feathers, hair, horns, leather, metal, paints (excluding any boiling process), paper, textiles.

Manufacturing, compounding, processing, canning or packaging of products such as bakery goods, candy and soft drinks, dairy products, food products (excluding fish and meat products, sauerkraut, vinegar, yeast, and the rendering or refining of fats and oils).

Mattress manufacture, repair, rebuildings and recovering.

D. Other uses:

Agricultural supplies and equipment, sales and service.
Agricultural uses, but excluding dairies, stockyards, slaughter of animals, and manufacture of fertilizer.
Automobile accessory and parts sales.
Automobile repair services; no open service bays shall face a public street, or they shall be screened.
Automobile sales, new and used.
Barbershops.
Boat, mobilehome and camper sales and services.
Building material and hardware sales.
Catering services.
Cleaning and dyeing plants, laundries, linen and towel service.
Creameries.
Electric distribution substations, electric transmission substations, and public utility buildings and service yards.
Furniture upholstery.

Ice manufacture and storage, frozen food lockers, and cold storage plants.
Lumberyards (no planing mills).

E. Machine shops and such uses as the following:

Anodizing shops.
Blacksmith shops.
Cabinet or carpenter shops.
Die and pattern making shops.
Electroplating shops.
Grinding shops.
Metal engraving shops.
Metal finishing and plating shops.
Polishing shops.
Sheet metal shops.
Tinsmith shops.
Welding shops.
Parking lots, commercial.
Petroleum bulk plants.
Plumbing, heating or electrical shops.
Real estate, business and professional offices.
Repair and fix-it shops.
Repair garages, body and fender works and auto painting, providing all work is conducted within a completely enclosed structure.
Retreading and recapping of tires.
Service stations.
Sign painters.
Taxidermy shops.
Tree surgeons.
Volume sales outlets, such as furniture, appliances and carpeting.
Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).
Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.
Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.
Wholesaling."

SECTION 5. Redlands Municipal Code Section 18.108.050, entitled "Conditional Uses" for the Light Industrial (M-1) District, is hereby amended to read as follows:

"The following uses may be permitted in the M-1 zone subject to approval of a conditional use permit:

Animal and pet hospitals, kennels and animal pounds.
Automobile wash, mechanical or self-service.

Building materials storage yards.
Business, technical, trade or professional schools.
Commercial recreation such as bowling lanes and skating rinks.
Contractors' storage yards.
Equipment rentals.
Feed and fuel yards.
Motels.
Outdoor vehicle storage and holding lot, with no dismantling or wrecking permitted.
Restaurants.
~~Warehouses and logistics distribution centers, in accordance with chapter 18.156 of this title.~~"

SECTION 6. Redlands Municipal Code Section 18.112.030, entitled "Permitted and Accessory Uses" for the Industrial (I-P) District, is hereby amended to read as follows:

"18.112.030: PERMITTED AND ACCESSORY USES:

Principal permitted uses in the I-P zone include:

A. Accessory uses:

Commercial sales and service incidental to a principal permitted use.

Employee recreational facilities and play areas.

One dwelling unit on the same parcel of land as a permitted use needing continual supervision, to be occupied exclusively by a superintendent or a caretaker and his family.

Storage buildings incidental to a permitted use.

Other accessory uses and buildings customarily appurtenant to a permitted use.

B. Manufacturing:

Machine tool manufacture, including metal lathes, presses and stamping machines, and woodworking machines.

Machinery manufacture, including electrical, agricultural, construction, mining, air conditioning equipment, dishwashers, dryers, furnaces, heaters, stoves and washing machines.

Manufacture of chemicals and chemical products, except those requiring a conditional use permit.

Manufacture of food products, including such processes as cooking, roasting, refining and extraction involved in the preparation of such products as cereal, chocolate, cider, coffee, glucose, rice, flour, feed and grain, vegetable oils and yeast; but not including fish or meat products.

Manufacturing and processing of the following, conducted in an enclosed building, except that any outdoor manufacturing or processing operation in this group of uses shall be subject to approval of a conditional use permit:

Abrasives.

Aircraft and aircraft accessories.

Aluminum products.

Asbestos.

Automobiles, trucks and trailers.

Automotive accessories and parts.

Boats.

Candles.

Canvas.

Carpets and rugs.

Cellophane.

Cloth.

Composition wallboard.

Cork.

Felt.

Fiber.

Fur.

Glass, but excluding blast furnaces.

Glazed tile.

Hemp products.

Ink.

Jute products.

Leather.

Linter.

Metal foil.

Metal products.

Missiles and missile components, excluding explosive fuels.

Motors and generators.

Paper.

Plastics.

Porcelain products.

Pulp goods.

Putty.

Railroad equipment.

Rubber products.

Sisal products.

Starch and dextrine.

Structural steel products.

Textiles.

Tile.

Wire and wire products.

Yarns.

Metal fabricating, heat treating, pickling and stamping.

Transit and transportation terminals, repair and storage facilities.

C. Services:

Blueprinting, photocopying and film processing.

Business and research offices related to the administration and operation of the permitted industrial uses.

Electrical distribution substations, electrical transmission substations, public utility service yards and steam electric generating stations.

Laboratories.

Lumberyards.

Newspaper publishing.

Off street parking.

Offices, business and professional.

Petroleum bulk plants.

Printing, lithographing, publishing.

Public buildings.

Public utility offices.

Radio and television broadcasting.

Restaurants operated for employees on the premises.

Trade union halls.

Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.

Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).

Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.

Wholesaling."

SECTION 7. Redlands Municipal Code Section 18.112.050, entitled "Conditional Uses" for the Industrial (I-P) District, is hereby amended to read as follows:

"The following uses may be permitted subject to approval of a conditional use permit:

A. Heliports.

B. Manufacturing of:

Acetylene.
Ammonia.
Aniline dyes.
Bleaching powder.
Breweries, distilleries and wineries.
Bronze, babbitt metal and similar alloys.
Carbide.
Carbolic, hydrochloric, picric and sulfuric acid.
Caustic soda.
Cellulose and celluloid.

Chlorine.
Coal, coke or coal tar products.
Exterminating agents.
Film.
Gas.
Lacquer, shellac, turpentine, varnish or calcimine (Kalsomine).
Linoleum or oilcloth.
Matches.
Nitrating of cotton and other materials.
Phenol.
Potash.
Pyroxylin.
Rubber (natural or synthetic).
Soap, tallow, grease and lard.
Radio transmitter towers higher than fifty feet (50') above ground level.

C. Storage of:

Oil or gas in amounts of two thousand five hundred (2,500) barrels or more.
Oil or gas within three hundred feet (300') of any residential zone, school or park.
Recreational vehicles and boats.

~~D. Warehouses and logistics distribution centers, in accordance with chapter 18.156 of this title.~~

D. Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid conditional use permit approved prior to the effective date of Ordinance No. 3002). Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title."

SECTION 8. Redlands Municipal Code Section 18.116.030, entitled "Permitted Uses" General Industrial (M-2) District, is hereby amended to read as follows:

"18.116.030: PERMITTED USES:

Principal permitted uses in the M-2 zone include:

A. Uses permitted in the M-1 industrial zone.

B. Contractors' yards and shops, including building, masonry, painting, concrete, electrical, plumbing, refrigeration, roofing, heating and air conditioning.

C. Electrical distribution substations, electrical transmission substations, nonnuclear electric generating stations, and public utility buildings, office, and service yards, and steam electric generating stations.

D. Food products manufacture, including such processes as cooking, roasting, refining and extraction involved in the preparation of such products as cereal, chocolate, cider, coffee, glucose, rice, flour, feed and grain, vegetable oils and yeast; but not including fish or meat products.

E. Lumberyards, lumber processing and woodworking, including planing mills, plywood, veneering, wood preserving and laminating.

F. Machine tool manufacture, including metal lathes, presses and stamping machines, and woodworking machines.

G. Machinery manufacture, including electrical, agricultural, construction, mining, air conditioning equipment, dishwashers, dryers, furnaces, heaters, stoves and washing machines.

H. Manufacture of chemicals and chemical products, except those requiring a conditional use permit.

I. Manufacture, storage, reconditioning and exchange of such items as cans, containers, boxes, barrels, bottles and bags.

J. Manufacturing and processing of the following, conducted in an enclosed building, except that any outdoor manufacturing or processing operation in this group of uses shall be subject to approval of a conditional use permit:

Abrasives.
Aircraft and aircraft accessories.
Aluminum products.
Asbestos.
Automobiles, trucks and trailers.
Automotive accessories and parts.
Boats.
Bricks.
Burial vaults and caskets.
Candles.
Canvas.
Carpets and rugs.
Cement products.
Chalk.
Clay pipe and clay products.
Composition wallboard.
Glass, but excluding blast furnaces.
Glazed tile.
Graphite and graphite products.
Hemp products.
Ink.
Jute products.

Linter.
Metal foil.
Metal products.
Missiles and missile components, excluding explosive fuels.
Motors and generators.
Paraffin products.
Plastics.
Porcelain products.
Pulp goods.
Pumice.
Putty.
Railroad equipment.
Rubber products.
Sand and lime products.
Sisal products.
Starch and dextrine.
Steel products.
Stone products.
Structural steel products.
Tile.
Wire and wire products.

K. Metal fabricating, heat treating, pickling and stamping.

L. Storage facilities, except those requiring a conditional use permit.

M. Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).

N. Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.

O. Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid land use entitlement approved prior to the effective date of Ordinance No. 3002). Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title."

SECTION 9. Redlands Municipal Code Section 18.116.050, entitled "Conditional Uses" General Industrial (M-2) District, is hereby amended to read as follows:

"In the M-2 zone, the following uses may be permitted subject to approval of a conditional use permit:

A. Airports, heliports and landing strips.

B. Animal, food or beverage processing of the following kinds:

Breweries, distilleries and wineries.
Meat or fish products packing, canning or processing.
Vinegar, yeast and sauerkraut.

C. Asphalt, concrete and earth products activities of the following kinds:

Asphalt batching plants.
Concrete mixing and batching plants.
Rock crushing plants and aggregate dryers.
Sandblasting plants.
Butane service and filling stations.

D. Commercial and service type uses which the commission, after study and deliberation, finds are needed to serve the M-2 district, and which will not interfere with the orderly development of the industrial area, and which will be compatible with industrial uses.

E. Distilling of:

Alcohol.
Bones.
Coal.
Coal tar.
Coke.
Wood.
Heavy metal works of the following kinds:
Blast furnaces.
Boiler works.
Drop forge industries.
Drop hammers.
Forges, foundries and forging works.
Metal and metal ore reduction or smelting.
Rolling mills.

F. Manufacturing of:

Acetylene.
Ammonia.
Aniline dyes.
Asphalt or asphalt products.
Bleaching powder.
Bronze, babbitt metal and similar alloys.
Carbide.
Carbolic, hydrochloric, picric and sulfuric acid.
Caustic soda.
Cellophane.

Cellulose and celluloid.
Cement, lime, gypsum or plaster of Paris.
Charcoal, lampblack or fuel briquettes.
Chlorine.
Coal, coke or coal tar products.
Creosote.
Exterminating agents.
Fertilizer.
Film.
Gas.
Lacquer, shellac, turpentine, varnish or calcimine (kalsomine).
Linoleum or oilcloth.
Matches.
Nitrating of cotton and other materials.
Phenol.
Potash.
Pyroxylin.
Rubber (natural or synthetic).
Soap, tallow, grease and lard.
Radio transmitter towers, higher than fifty feet (50') above ground level.

G. Refining of:

Fats and oils.
Metals and metal ores.
Petroleum and petroleum products.
Sugar.
Salvage, wrecking and disposal activities of the following kind:
Automobile wrecking and salvage.
Building wrecking and salvage.
Dumps, including garbage and trash disposal.
Industrial waste material salvage, waste metal, rag, clothing, glass and paper salvage operations.
Sewer farm or sewage disposal plants.

H. Storage of:

Automobiles and other vehicles purchased for wrecking operations.
Fertilizer or manure.
House movers' equipment and buildings moved from other locations.
Oil or gas in amounts of two thousand five hundred (2,500) barrels or more.
Oil or gas within three hundred feet (300') of any residential zone, school or park.
Sand, gravel, rock or decomposed granite in amounts of two thousand (2,000) tons or more.
Used building materials or secondhand buildings.

~~I. Warehouses and logistics distribution centers, in accordance with chapter 18.156 of this title.~~"

SECTION 10. Chapter 18.156 of the Redlands Municipal Code, entitled "Development Provisions for Specific Uses," Article XII entitled "Warehouses and Logistics Distribution Centers," is hereby amended as follows:

"ARTICLE XII. Warehouses and Logistics Distribution Centers

18.156.900: DEFINITIONS:

ALTERATION:	Any construction or renovation to an existing structure other than repair or addition. A change, addition or modification in construction, change in occupancy or use, or structural repair to an existing building or facility. Alterations include, but are not limited to, remodeling, renovation, rehabilitation, reconstruction, historic restoration, resurfacing of interior circulation paths or vehicular ways, changes or rearrangement of the structural parts or elements, and changes or rearrangement in the plan configuration of walls and full-height partitions. Normal maintenance, reroofing, painting or wallpapering, or changes to mechanical and electrical systems are not alterations unless they affect the usability of the building or facility.
REPAIR:	*Repair* has the same meaning as defined in the California Building Code (Chapter 2, as amended, California Building Code).
WAREHOUSE:	Warehouse/distribution facilities primarily used for the storage and/or consolidation of manufactured goods before their distribution to retail locations or other warehouses. Warehouse/distribution centers are fifty thousand (50,000) square-feet or more in gross floor area or contain six (6) or more truck docks or dock high loading doors. They are characterized by dock high loading doors and could be on opposing sides of the building (cross dock facility); may include grade-level loading doors; interior clear heights a minimum of 28 to 36 feet to ceiling for the warehousing floor area; significant movement and storage of products, materials, or equipment; may include receiving, sorting, re-packaging, and/or re-distribution; truck activities frequently outside of the peak hour of the adjacent street system; and need freeway access. This definition excludes facilities owned and operated by a government agency or any public or private utilities. Warehousing and distribution facilities include, but are not limited to, the following types of uses: A. Warehousing distribution/high cube distribution centers. B. Parcel delivery terminals or truck terminals. C. Parcel sorting and distribution facilities. D. Package allocation for delivery drivers or independent delivery contractors. E. Parcel hub or high cube fulfillment center. F. Freight yards or forwarding terminals.

	G. Moving agencies. H. Shipping/receiving yards.
WAREHOUSING, ANCILLARY:	The use of a portion of a building for the related storage of goods of any type by one or two businesses and used for the sale or distribution of those goods directly to their customers. A manufacturing, assembly, service commercial, or other type of commercial or industrial use (i.e., primary use) manufactures and/or stores and distributes the goods or components that are produced or contained on-site, and therefore includes the related storage of those goods or items. Ancillary storage or warehousing is subordinate and incidental to the primary land use (e.g., manufacturing, assembly, service commercial, or other type of primary commercial or industrial use). Ancillary storage or warehousing may include ground level loading doors on one or more sides of the building, or not more than five (5) dock high loading doors on one side of the building only.

18.156.910: APPLICABILITY:

The provisions of this section shall apply to the following types of development projects:

A. New warehouse development projects that meet one of the following criteria (note: excludes government agency facilities and public or private utility facilities).

1. Gross floor area of fifty thousand (50,000) square-feet or more; or,
2. A structure with six (6) or more truck docks or dock high loading doors (does not include grade-level loading doors or loading spaces).

~~B. Development or r edevelopment projects for existing or proposed warehouse facilities involving demolition, reconstruction, repairing, or rebuilding that exceed fifty percent (50%) of the reasonable replacement value of the existing structure or property.~~

1. ~~Estimates for this purpose shall be reviewed and approved by the building official and the Development Services Director, or their respective designees, and shall be based on the minimum cost of construction in compliance with the California Building Code.~~
2. ~~For the purpose of this section, "assessed value" shall mean the assessed value of the structure as shown on the County of San Bernardino property assessment roll in effect at the time of the occurrence of the casualty, or at the time the repair and maintenance is first conducted.~~
3. ~~Redevelopment of a property and/or building shall include the feasible provisions of Section 18.156.930 through 18.156.960 of this Article, as determined by the Planning Commission (the location requirements of Section 18.156.920 shall not apply to redevelopment projects).~~

~~C.~~ B. Required Compliance. No new warehouse development project shall be constructed, no redevelopment or reconstruction of a property for warehouse use, and no existing warehouse shall be moved, altered, or enlarged, except in accordance with the applicable development standards of this Article and/or applicable State law. If any provisions of this article conflict or are inconsistent with applicable State law, then State law shall prevail.

C. A property with a valid unexpired land use entitlement for a new warehouse or logistics distribution facility that has not yet been constructed or established as of the effective date of Ordinance No. 3002 shall have the same land use rights as if the structure had been existing on the effective date of Ordinance No. 3002.

18.156.920: SITE LOCATION REQUIREMENT:

A. No warehouses shall be located on a project site more than one mile (5,280 feet) from a freeway entrance/exit ramp to the Interstate Freeway System (Interstate 10 and Interstate 210). For purposes of this requirement, the linear distance shall be measured as a radius from a freeway ramp to any part of the subject property.

B. Assemblage of Parcels Prohibited: No warehouse development project, or redevelopment or reconstruction of a property for warehouse use, may assemble or merge additional properties for the purpose of developing, enlarging, expanding, or intensifying the use of an existing warehouse or logistics distribution facility.

18.156.930: SCREENING AND BUFFERING REQUIREMENTS:

A. Warehouse developments shall provide a solid decorative wall(s) of at least ten feet (10') in height when abutting any of the following land uses: any residence including private homes, condominiums, apartments, and living quarters; schools and preschools; daycare centers and in-home daycares; hospitals; long-term care facilities; retirement and nursing homes; community centers; places of worship; parks (excluding trails); and dormitories. The exterior treatment of the wall(s) shall be decorative or painted.

B. Unless physically impossible, loading docks and truck entries shall be oriented away from abutting sensitive receptors. To the greatest extent feasible, loading docks, truck entries, and truck drive aisles shall be located away from nearby sensitive receptors. In making feasibility decisions, the City must comply with existing laws and regulations and balance public safety and the site development's potential impacts to nearby sensitive receptors. Therefore, loading docks, truck entries, and drive aisles may be located nearby sensitive receptors at the discretion of the Planning Commission, but any such site design shall include measures designed to minimize overall impacts to nearby sensitive receptors.

C. Trees shall be used as part of the solid screen buffering treatment for any adjacent residential properties or properties with sensitive receptors. Trees used for this

purpose shall be evergreen, drought-tolerant, minimum 36-inch box size, and shall be spaced no greater than 40-feet on center. Palm trees shall not be used for screening purposes. The property owner and any successors in interest shall maintain these trees for the duration of ownership ensuring any unhealthy or dead trees are replaced timely as needed.

D. Trees shall be installed in automobile (passenger vehicle) parking areas to provide at least thirty five percent (35%) shade cover of parking areas within fifteen (15) years. This requirement is in addition to the applicable standard design requirements for parking lot landscape and related improvements. Trees shall be planted that are capable of implementing this requirement.

18.156.940: TRAFFIC PATTERNS AND SIGN REQUIREMENTS:

A. Applicants for entitlements shall prepare and submit a Truck Routing Plan demonstrating the most direct route(s) to and from the Interstate Freeway System based on the city's latest Truck Route Map. Routes to or from freeway ramps shall not pass through any residential zones or districts.

B. A traffic impact assessment (TIA) report shall be prepared to evaluate a proposed warehouse project's compliance with the City's Measure U traffic system requirements, and shall include an evaluation of the City's streets and Truck Routes that provide vehicular access to the Interstate Freeway System, including, but not limited to: existing right-of-way width; roadway capacity to handle the proposed quantity of truck trips to be generated by the proposed use (including any road widening that may be necessary); roadway design and improvements to handle the weight and frequency of proposed truck trips; intersection operations to freeway ramps and level of service analysis to include the proposed truck trips; truck turn radii at intersections; and other operational elements of the City's street network to serve the proposed use. The TIA may be prepared by a qualified consultant selected and directed by the City (and all consultant costs to be reimbursed by the applicant), or by a qualified traffic consultant selected by the applicant (and all work subject to the direction, review, and approval by the City).

C. Entry gates into the loading dock/truck court area with more than 20 loading docks shall be positioned after a minimum of 140 feet of total available stacking depth inside the property line (or alternatively, if 140 feet of depth is not feasible due to site constraints, then provide 70 feet of available stacking depth for two trucks side-by-side as an alternative design). The stacking distance shall be increased by 70 feet for every 20 loading docks beyond 50 docks. Queuing, or circling of vehicles, on public streets immediately pre- or post-entry to an industrial commerce facility is strictly prohibited unless queuing occurs in a deceleration lane or right turn lane exclusively serving the facility.

D. Prior to entitlement approval, applicants shall submit to the City, and obtain approval of, all turning templates to verify adequate truck turning movements at entrance and exit driveways as well as street intersections adjacent to industrial

buildings. Unless not physically possible, truck entries shall be located on Collector streets or streets of a higher commercial classification, and vehicle entries shall be designed to prevent truck access on streets that are not Collector Streets (or streets of a higher commercial classification), including but not limited to by limiting the width of vehicle entries.

E. Anti-idling signs indicating a five (5) minute restriction on engine idling for diesel trucks shall be posted at warehouses and industrial commerce facilities along entrances to the site and within the dock areas and shall be strictly enforced by the facility operator (13 CCR § 2480).

F. Signs shall be installed at all truck exit driveways directing truck drivers to the truck route as indicated in the Truck Routing Plan to be routed to the Interstate Freeway System.

G. Signs and drive aisle pavement markings shall clearly identify the onsite circulation pattern to minimize unnecessary on-site vehicular travel.

H. Facility operators shall post signs in prominent locations inside and outside of the building indicating that off-site parking for any Medium Heavy-Duty trucks, Heavy Heavy-Duty trucks, truck trailers or cabs, and other operations-related vehicles is strictly prohibited. City may require facility operator to post signs on adjacent and nearby surface or residential streets indicating that off-site truck parking is prohibited by City ordinance.

I. All signs under this Section shall be legible, durable, and weather-proof.

18.156.950: SUSTAINABLE ENERGY:

A. A minimum of ninety percent (90%) of the on-site motorized operational equipment shall be zero emission (ZE).

B. All warehouse building roofs shall install photovoltaic (PV) solar collector system or other form of on-site renewable energy, provided such renewable energy source is recognized by the State of California as a renewable resource under the Renewable Portfolio Standard Program. The renewable energy system shall be metered separately from the nonrenewable metered power usage of the building (if not in conflict with other applicable regulations). The renewable energy system shall be built to generate an amount of electricity sufficient to meet the following criteria:

1. Annualized building demand based on the approved use or, if no use is proposed, then the demand for the most energy intensive use that could occupy the building; and

2. Annualized demand required to charge fully electric vehicles and trucks, assuming that all vehicles and trucks to the site are fully electric; and

3. A reasonable rate of efficiency loss over ten years.

Note: Electricity demand that exceeds the generation capacity of the on-site renewable energy system may be obtained from off-site energy sources or suppliers.

C. The warehouse building's rooftop that is not covered with solar panels or other utilities shall be constructed with light colored roofing material with a solar reflective index (SRI) in accordance with current California Energy Code regulations. This material shall be the minimum solar reflective rating of the roof material for the life of the building.

D. The on-site passenger vehicle parking shall include electric vehicle (EV) ready parking spaces in accordance with current requirements of the California Building Code, and at least fifty percent (50%) of the required EV parking spaces shall be equipped with working Level 2 Quick Charge EV charging stations installed and operational, prior to building occupancy. Signage shall be installed indicating EV charging stations and specifying that spaces are reserved for clean air/EV vehicles. Unless superior technology is developed that would replace the EV charging units, facility operator and any successors in interest shall be responsible for maintaining the EV charging stations in working order for the life of the facility.

E. Unless the owner of the facility records a covenant on the title of the underlying property ensuring that the property cannot be used to provide chilled, cooled, or freezer warehouse space, a conduit shall be installed during construction of the building shell from the electrical room to all (100%) of the loading dock doors that have potential to serve the refrigerated space. When tenant improvement building permits are issued for any refrigerated warehouse space, electric plug-in units shall be installed at every dock door servicing the refrigerated space to allow transport refrigeration units (TRUs) to plug in. Truck operators with TRUs shall be required to utilize electric plug-in units when at loading docks.

18.156.960: OPERATION AND CONSTRUCTION:

A. Cool surface treatments shall be added to all drive aisles and parking areas, or such areas shall be constructed with a solar-reflective cool pavement such as concrete. Solar collectors may be installed on support structures that provide shade over parking areas to achieve minimum requirements.

B. To ensure that warehouse electrical rooms are sufficiently sized to accommodate the potential need for additional electrical panels, either a secondary electrical room shall be provided in the building, or the primary electrical room shall be sized twenty-five percent (25%) larger than is required to satisfy the service requirements of the building or the electrical gear shall be installed with the initial construction with 25% excess demand capacity.

C. All exterior light fixtures (including but not limited to parking lot lighting, wall fixtures, roof fixtures, light poles, etc.) visible from public right-of-way or abutting properties shall have shielding affixed to contain illumination within the subject property and prevent light trespass and glare overspill.

D. The facility operator shall be required to perform regular maintenance of building structures, landscaping, and paved surfaces to ensure good physical condition and appearance.

E. For any sites with warehouses that are abutting or adjacent to any residential properties or properties containing sensitive receptors, any outdoor storage of materials, high-pile storage, or any other manner of storage or staging shall not exceed the height of the perimeter wall.

F. Additional operating conditions may be enacted for an individual Warehouse project pursuant to a Conditional Use Permit (~~RMC~~ Redlands Municipal Code Chapter 18.192) for the purpose of avoiding or reducing potential off-site nuisance effects of the warehouse facility (including but not limited to traffic, parking, noise, vibration, air quality emissions, etc.) on nearby sensitive receptors or residential districts, or to protect the public health, safety, or general welfare."

SECTION 11. Redlands Municipal Code Chapter 18.156, Article XII entitled "Warehouses and Logistics Distribution Centers," is hereby amended to add Section 18.156.970 as follows:

"18.156.970: REBUILDING PROVISIONS FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION CENTERS:

A. For warehouses and logistics distribution facilities existing as of the effective date of Ordinance No. 3002, the criteria for alterations or repairs to the existing structure or property are as follows:

1. Ordinary repair and maintenance may be performed on a structure or property subject to the provisions of this article, and in accordance with applicable law (e.g., California Building Code, California Fire Code, etc.).

2. Improvements to the existing structure including technology upgrades (e.g., seismic strengthening, energy use efficiency, PV solar or re-roof, water use efficiency, reductions to greenhouse gas emissions, hazardous materials remediation, etc.) may be installed on a structure or property subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

3. Warehouses and logistics distribution facility buildings may be voluntarily rebuilt, reconstructed, or otherwise altered, subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

4. If the warehouse or logistics distribution facility building is involuntarily damaged or destroyed by natural disasters (i.e., fire, flood, earthquake or other calamity or acts of God), the entirety of the structure may be rebuilt subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

B. Existing warehouses and logistics distribution facilities (existing as of the effective date of Ordinance No. 3002) may be rebuilt to the previously existing square-footage (building footprint), previously existing height, and previously existing number of truck docks if the subject property meets the following criteria:

1. The warehouse or logistics distribution use was legally established prior to the effective date of Ordinance No. 3002; or if not yet established, the subject property had a valid land use entitlement issued prior to the effective date of Ordinance No. 3002.

2. The Development Services Director has determined the existing business to be a permitted or conditionally permitted use.

3. An applicable building permit(s) shall be obtained for reconstruction, if required.

4. A change in ownership or tenancy without any change in use or occupancy shall not affect any of the rebuilding rights, privileges, and responsibilities provided pursuant to this section.

5. It shall be the property owner's responsibility to provide evidence or information to justify the establishment of rebuilding rights.

C. Existing warehouses and logistics distribution facilities (existing as of the effective date of Ordinance No. 3002) may be altered and request an increase to the building height pursuant to the following criteria:

1. ~~Interior ceiling height~~ Building height may be increased up to ~~15% (and overall building height not to exceed~~ the maximum height allowable within the applicable land use district (or 50 feet if no maximum is specified) ~~or an applicable entitlement)~~ to incorporate technology upgrades, energy efficiency improvements, or other justifiable economic or environmental reasons; and/or may increase the number of previously existing truck dock positions; provided the structure meets the criteria listed below.

a. The subject property meets all applicable criteria in Section 18.156.970(B).

b. The subject property obtains a Conditional Use Permit issued pursuant to Chapter 18.192 of this title.

c. Construction or redevelopment of a building involving additional height shall include the feasible provisions of Section 18.156.930 through 18.156.960 of this article, as determined by the Planning Commission (the location requirements of Section 18.156.920(A) shall not apply). For purposes of this article, “feasible” has the same meaning as California Code of Regulations Title 14, § 15364.

d. Complete an environmental review process, if applicable, in accordance with the California Environmental Quality Act for a proposed project that will increase building height, increase the number of truck docks, or change non-refrigerated space to refrigerated space.

e. The applicant shall prepare and submit ~~commission may require one or more of~~ the following in conjunction with a development application for a land use entitlement: ~~in instances where the proposed redevelopment, reconstruction, or alteration appears to create impacts to traffic, landscaping, or economic feasibility:~~

i. Circulation studies, prepared by a traffic engineer, showing the movement of vehicular and truck traffic to and from the subject property, and to and from existing thoroughfares. Special engineering features and/or traffic regulation devices needed to facilitate or ensure safety of circulation may be required.

ii. A landscaping and tree planting plan, prepared by a landscape architect.

iii. An economic feasibility report or market analysis, prepared by a qualified economist, justifying the need to increase the building height and/or increase the number of truck docks.

iv. An energy audit analysis report to identify current (baseline) conditions for the existing structure; and an energy analysis for the proposed modified facility to demonstrate compliance with the California Building Code and that there will be a demonstrated improvement to energy efficiency."

SECTION 12. Severability. If any section, subsection, subdivision, sentence, clause, phrase, or portion of this Ordinance for any reason is held to be invalid or unconstitutional by the decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this Ordinance. The City Council hereby declares that it would have adopted this Ordinance, and each section, subsection, subdivision, sentence, clause, phrase, or portion thereof, irrespective of the fact that any one or more sections, subsections, subdivisions, sentences, clauses, phrases, or portions thereof be declared invalid or unconstitutional.

SECTION 13. The Mayor shall sign this ordinance and the City Clerk shall certify to the adoption of this ordinance and shall cause it, or a summary of it, to be published once in a newspaper of general circulation within the City, and thereafter, this ordinance shall take effect as provided by law.

ADOPTED, SIGNED AND APPROVED this ___ day of _____, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk, City of Redlands, hereby certify that the foregoing Ordinance was duly adopted by the City Council at the regular meeting thereof, held on the ___ day of _____, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

ORDINANCE NO. 3002

AN ORDINANCE OF THE CITY OF REDLANDS AMENDING TITLE 18 (ZONING REGULATIONS) OF THE REDLANDS MUNICIPAL CODE TO PROHIBIT NEW WAREHOUSING AND LOGISTICS DISTRIBUTION CENTERS, AS DEFINED, IN THE COMMERCIAL AND INDUSTRIAL ZONES, WHILE ALLOWING FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION USES TO REMAIN AS PERMITTED OR CONDITIONALLY PERMITTED USES SUBJECT TO NEW REBUILD PROVISIONS.

WHEREAS, the City Council of the City of Redlands has initiated Ordinance Text Amendment No. 372, in accordance with Chapter 18.204 (Amendments) of the Redlands Municipal Code, as the public necessity, convenience, or general welfare justifies such action; and

WHEREAS, over the past twenty years, Redlands has experienced the construction of numerous large warehouses and logistics distribution facilities in and around the City of Redlands including the unincorporated County jurisdiction located in northwest Redlands; and

WHEREAS, on September 29, 2024, the Governor of the State of California signed Assembly Bill (AB) 98 to add Section 65302.02 to, and to add Chapter 2.8 (commencing with Section 65098) to Division 1 of Title 7 of, the Government Code, and to add Sections 40458.5 and 40522.7 to the Health and Safety Code, relating to land use, and the "Warehouse Concentration Region" defined therein includes the City of Redlands among other nearby cities and counties; and

WHEREAS, two major transportation corridors (Interstate 10 and Interstate/S.R. 210 freeways) serve the Southern California region and are gateways to the Interstate Highway System, and both freeways pass through the City of Redlands, which contributes to a significant quantity of heavy-truck and other vehicular traffic to pass through the City to reach destinations located outside the City of Redlands as well as within the unincorporated "donut hole" area; and

WHEREAS, heavy-truck traffic that serves several million square feet of warehousing and logistics distribution uses located within the unincorporated County island area (surrounded by the City of Redlands) must pass through the City and utilize City streets on a daily basis at all hours of the day and night; and

WHEREAS, the residents and visitors of the City of Redlands may experience exposure to environmental effects (such as numbers of truck trips, vehicle miles traveled, greenhouse gas emissions affecting air quality, vehicular noise, etc.) and other externalities from such warehousing and logistics distribution uses; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about March 24, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on April 14, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about April 21, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on May 12, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, the proposed Ordinance No. 3002 is exempt from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines; and

WHEREAS, following the public hearing on May 12, 2026, the Planning Commission determined that Ordinance Text Amendment No. 372 would be in conformity with the 2035 General Plan, and would be consistent with goals of the General Plan for transportation, connectivity, compatibility and harmonious relationship of different land uses; and

WHEREAS, on May 12, 2026, the Planning Commission recommended approval of Ordinance Text Amendment No. 372 to the City Council; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, the City Clerk gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by City Council; and

WHEREAS, on June 16, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing; and

WHEREAS, on September 1, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing; and

WHEREAS, on September 1, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and continued the public hearing to October 6, 2026; and

WHEREAS, on October 6, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF REDLANDS DOES ORDAIN AS FOLLOWS:

SECTION 1. California Environmental Quality Act. The proposed Ordinance Text Amendment does not require environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section 15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the zoning code amendment may have a significant effect on the environment, insofar as it would amend the lists of permitted land uses in the City of Redlands. Furthermore, even if the proposal is considered a project, the proposed zoning code amendment is categorically exempt under CEQA Guidelines Section 15308, because it is clear that it will not create an environmental impact and the action will assure the maintenance, enhancement, or protection of the environment through the adoption of regulations prohibiting new large new warehouses and logistics distribution facilities. Accordingly, no further environmental review is necessary.

SECTION 2. Redlands Municipal Code Section 18.100.040, entitled "Permitted Uses" for the Commercial Industrial (C-M) District, is hereby amended to read as follows:

"18.100.040: PERMITTED USES:

Principal permitted uses in the C-M zone include:

A. Auto services: No open service bays shall face a public street, or they shall be screened:

Brake relining.
Glass installation.
Muffler installation.
Painting.
Repair.
Upholstery.

B. Commercial sales and service:

Agricultural supplies and equipment.
Automobile equipment.
Automobile, new and used.
Bicycle, boat and motorcycle.
Building material and hardware.
Cabinet shop.
Camper and mobilehome.
Drive-in stores, such as milk and food, no alcohol beverage sales.
Electrical apparatus and equipment.
Furniture, appliances and carpeting.

Garden and farm supplies.
Interior decorator studios.
Machinery, equipment and supplies.
Nurseries; no outdoor display of merchandise other than plants.
Office equipment.
Paint.
Pet and pet supply.
Plumbing, heating, air conditioning and refrigeration equipment and supplies.
Radio, television and musical instruments.

C. Industrial:

Uses permitted in the M-P planned industrial district.

Recreation and entertainment: The following uses are subject to approval of a conditional use permit if within three hundred feet (300') of a residential area:

Bowling lanes, skating rinks, and sports arenas, no alcohol beverage sales.
Drive-in theaters.

D. Services:

Auction houses.
Auto rental.
Bus terminals and similar transit facilities.
Cleaning and dyeing plants, laundries, linen and towel service.
Furniture upholstery.
Governmental agencies.
Ice manufacture, cold storage, and frozen food lockers.
Mail order houses.
Motels and hotels.
Parcel delivery.
Pest control.
Public scales.
Radio and television broadcasting studios.
Restaurants.
Retreading of tires.
Sign painters.

E. Other uses:

Agricultural uses permitted in the M-P district.
Business, technical, trade or professional schools.
Clubs, lodges, and similar organizations.
Electric distribution substations, public utility buildings and service yards.
Van and storage.

Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).
Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.
Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.
Wholesalers."

SECTION 3. Redlands Municipal Code Section 18.100.070, entitled "Conditional Uses" for the Commercial Industrial (C-M) District, is hereby amended to read as follows:

"18.100.070: CONDITIONAL USES:

The following uses may be permitted in the C-M zone subject to approval of a conditional use permit:

Uses listed in chapter 18.192 of this title.
Ambulance service.
Animal hospitals.
Bowling lanes, skating rinks, and sports arenas, with alcohol beverage sales.
Cocktail lounges and bars.
Drive-in stores, such as milk and food, with alcohol beverage sales.
Equipment rental.
Radio and television transmitter towers higher than fifty feet (50') above ground level.
Regional shopping center containing at least one department store and a minimum gross land area of thirty five (35) acres; uses permitted shall be limited to those contained in the C-3 zone.
Retail store containing a minimum gross leasable area of seventy five thousand (75,000) square feet, subject to the parking requirements for neighborhood commercial districts.
Service stations."

SECTION 4. Redlands Municipal Code Section 18.108.030, entitled "Permitted and Accessory Uses" for the (M-1) Light Industrial District is hereby amended to read as follows:

"In the M-1 zone, principal permitted uses shall be as follows:

A. Uses permitted in the M-P, planned industrial district.

B. Accessory uses:

Commercial sales and service incidental to a principal permitted use.
Employee recreational facilities and play areas.
Storage buildings incidental to a permitted use.
Superintendent or caretaker dwelling. One dwelling unit on the same parcel of land as a permitted use needing continual supervision, to be occupied exclusively by a

superintendent or a caretaker and his family.
Other accessory uses and buildings customarily appurtenant to a permitted use.

C. Manufacturing:

Manufacture and assembly of electrical equipment and supplies, such as coils, condensers, lamps, switches, wire and cable assembly.

Manufacture of ceramic products, such as pottery, figurines and small glazed tile, utilizing only previously pulverized clay, and provided that kilns are fired only by electricity or gas.

Manufacture of cutlery, hardware, hand tools and kitchen utensils.

Manufacture, processing or treatment of products other than those which may be obnoxious or offensive by reason of emission of odor, dust, smoke, gas, noise, vibration or hazard.

Manufacturing, assembling, compounding, packaging and processing of articles or products from the following previously prepared materials: asbestos, bristles, bone, feathers, hair, horns, leather, metal, paints (excluding any boiling process), paper, textiles.

Manufacturing, compounding, processing, canning or packaging of products such as bakery goods, candy and soft drinks, dairy products, food products (excluding fish and meat products, sauerkraut, vinegar, yeast, and the rendering or refining of fats and oils).

Mattress manufacture, repair, rebuildings and recovering.

D. Other uses:

Agricultural supplies and equipment, sales and service.
Agricultural uses, but excluding dairies, stockyards, slaughter of animals, and manufacture of fertilizer.
Automobile accessory and parts sales.
Automobile repair services; no open service bays shall face a public street, or they shall be screened.
Automobile sales, new and used.
Barbershops.
Boat, mobilehome and camper sales and services.
Building material and hardware sales.
Catering services.
Cleaning and dyeing plants, laundries, linen and towel service.
Creameries.
Electric distribution substations, electric transmission substations, and public utility buildings and service yards.
Furniture upholstery.
Ice manufacture and storage, frozen food lockers, and cold storage plants.
Lumberyards (no planing mills).

E. Machine shops and such uses as the following:

Anodizing shops.
Blacksmith shops.
Cabinet or carpenter shops.
Die and pattern making shops.
Electroplating shops.
Grinding shops.
Metal engraving shops.
Metal finishing and plating shops.
Polishing shops.
Sheet metal shops.
Tinsmith shops.
Welding shops.
Parking lots, commercial.
Petroleum bulk plants.
Plumbing, heating or electrical shops.
Real estate, business and professional offices.
Repair and fix-it shops.
Repair garages, body and fender works and auto painting, providing all work is conducted within a completely enclosed structure.
Retreading and recapping of tires.
Service stations.
Sign painters.
Taxidermy shops.
Tree surgeons.
Volume sales outlets, such as furniture, appliances and carpeting.
Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).
Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.
Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.
Wholesaling."

SECTION 5. Redlands Municipal Code Section 18.108.050, entitled "Conditional Uses" for the Light Industrial (M-1) District, is hereby amended to read as follows:

"The following uses may be permitted in the M-1 zone subject to approval of a conditional use permit:

Animal and pet hospitals, kennels and animal pounds.
Automobile wash, mechanical or self-service.
Building materials storage yards.
Business, technical, trade or professional schools.

Commercial recreation such as bowling lanes and skating rinks.
Contractors' storage yards.
Equipment rentals.
Feed and fuel yards.
Motels.
Outdoor vehicle storage and holding lot, with no dismantling or wrecking permitted.
Restaurants."

SECTION 6. Redlands Municipal Code Section 18.112.030, entitled "Permitted and Accessory Uses" for the Industrial (I-P) District, is hereby amended to read as follows:

"18.112.030: PERMITTED AND ACCESSORY USES:

Principal permitted uses in the I-P zone include:

A. Accessory uses:

Commercial sales and service incidental to a principal permitted use.

Employee recreational facilities and play areas.

One dwelling unit on the same parcel of land as a permitted use needing continual supervision, to be occupied exclusively by a superintendent or a caretaker and his family.

Storage buildings incidental to a permitted use.

Other accessory uses and buildings customarily appurtenant to a permitted use.

B. Manufacturing:

Machine tool manufacture, including metal lathes, presses and stamping machines, and woodworking machines.

Machinery manufacture, including electrical, agricultural, construction, mining, air conditioning equipment, dishwashers, dryers, furnaces, heaters, stoves and washing machines.

Manufacture of chemicals and chemical products, except those requiring a conditional use permit.

Manufacture of food products, including such processes as cooking, roasting, refining and extraction involved in the preparation of such products as cereal, chocolate, cider, coffee, glucose, rice, flour, feed and grain, vegetable oils and yeast; but not including fish or meat products.

Manufacturing and processing of the following, conducted in an enclosed building, except that any outdoor manufacturing or processing operation in this group of uses shall be subject to approval of a conditional use permit:

Abrasives.

Aircraft and aircraft accessories.

Aluminum products.

Asbestos.

Automobiles, trucks and trailers.

Automotive accessories and parts.

Boats.

Candles.

Canvas.

Carpets and rugs.

Cellophane.

Cloth.

Composition wallboard.

Cork.

Felt.

Fiber.

Fur.

Glass, but excluding blast furnaces.

Glazed tile.

Hemp products.

Ink.

Jute products.

Leather.

Linter.

Metal foil.

Metal products.

Missiles and missile components, excluding explosive fuels.

Motors and generators.

Paper.

Plastics.

Porcelain products.

Pulp goods.

Putty.

Railroad equipment.

Rubber products.

Sisal products.

Starch and dextrine.

Structural steel products.

Textiles.

Tile.

Wire and wire products.

Yarns.

Metal fabricating, heat treating, pickling and stamping.

Transit and transportation terminals, repair and storage facilities.

C. Services:

Blueprinting, photocopying and film processing.

Business and research offices related to the administration and operation of the permitted industrial uses.

Electrical distribution substations, electrical transmission substations, public utility service yards and steam electric generating stations.

Laboratories.

Lumberyards.

Newspaper publishing.

Off street parking.

Offices, business and professional.

Petroleum bulk plants.

Printing, lithographing, publishing.

Public buildings.

Public utility offices.

Radio and television broadcasting.

Restaurants operated for employees on the premises.

Trade union halls.

Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title.

Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).

Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.

Wholesaling."

SECTION 7. Redlands Municipal Code Section 18.112.050, entitled "Conditional Uses" for the Industrial (I-P) District, is hereby amended to read as follows:

"The following uses may be permitted subject to approval of a conditional use permit:

A. Heliports.

B. Manufacturing of:

Acetylene.
Ammonia.
Aniline dyes.
Bleaching powder.
Breweries, distilleries and wineries.
Bronze, babbitt metal and similar alloys.
Carbide.
Carbolic, hydrochloric, picric and sulfuric acid.
Caustic soda.
Cellulose and celluloid.
Chlorine.
Coal, coke or coal tar products.
Exterminating agents.
Film.
Gas.

Lacquer, shellac, turpentine, varnish or calcimine (Kalsomine).
Linoleum or oilcloth.
Matches.
Nitrating of cotton and other materials.
Phenol.
Potash.
Pyroxylin.
Rubber (natural or synthetic).
Soap, tallow, grease and lard.
Radio transmitter towers higher than fifty feet (50') above ground level.

C. Storage of:

Oil or gas in amounts of two thousand five hundred (2,500) barrels or more.
Oil or gas within three hundred feet (300') of any residential zone, school or park.
Recreational vehicles and boats.

D. Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid conditional use permit approved prior to the effective date of Ordinance No. 3002). Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title."

SECTION 8. Redlands Municipal Code Section 18.116.030, entitled "Permitted Uses" General Industrial (M-2) District, is hereby amended to read as follows:

"18.116.030: PERMITTED USES:

Principal permitted uses in the M-2 zone include:

A. Uses permitted in the M-1 industrial zone.

B. Contractors' yards and shops, including building, masonry, painting, concrete, electrical, plumbing, refrigeration, roofing, heating and air conditioning.

C. Electrical distribution substations, electrical transmission substations, nonnuclear electric generating stations, and public utility buildings, office, and service yards, and steam electric generating stations.

D. Food products manufacture, including such processes as cooking, roasting, refining and extraction involved in the preparation of such products as cereal, chocolate, cider, coffee, glucose, rice, flour, feed and grain, vegetable oils and yeast; but not including fish or meat products.

E. Lumberyards, lumber processing and woodworking, including planing mills, plywood, veneering, wood preserving and laminating.

F. Machine tool manufacture, including metal lathes, presses and stamping machines, and woodworking machines.

G. Machinery manufacture, including electrical, agricultural, construction, mining, air conditioning equipment, dishwashers, dryers, furnaces, heaters, stoves and washing machines.

H. Manufacture of chemicals and chemical products, except those requiring a conditional use permit.

I. Manufacture, storage, reconditioning and exchange of such items as cans, containers, boxes, barrels, bottles and bags.

J. Manufacturing and processing of the following, conducted in an enclosed building, except that any outdoor manufacturing or processing operation in this group of uses shall be subject to approval of a conditional use permit:

Abrasives.
Aircraft and aircraft accessories.
Aluminum products.
Asbestos.
Automobiles, trucks and trailers.
Automotive accessories and parts.
Boats.
Bricks.
Burial vaults and caskets.
Candles.
Canvas.
Carpets and rugs.
Cement products.
Chalk.
Clay pipe and clay products.
Composition wallboard.
Glass, but excluding blast furnaces.
Glazed tile.
Graphite and graphite products.
Hemp products.
Ink.
Jute products.
Linter.
Metal foil.
Metal products.
Missiles and missile components, excluding explosive fuels.
Motors and generators.
Paraffin products.
Plastics.
Porcelain products.

Pulp goods.
Pumice.
Putty.
Railroad equipment.
Rubber products.
Sand and lime products.
Sisal products.
Starch and dextrine.
Steel products.
Stone products.
Structural steel products.
Tile.
Wire and wire products.

K. Metal fabricating, heat treating, pickling and stamping.

L. Storage facilities, except those requiring a conditional use permit.

M. Warehousing, ancillary to another primary use (see Redlands Municipal Code Chapter 18.156, Article XII).

N. Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors.

O. Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid land use entitlement approved prior to the effective date of Ordinance No. 3002). Such warehouse facilities shall be subject to the rebuild provisions contained in Section 18.156.970 of this title."

SECTION 9. Redlands Municipal Code Section 18.116.050, entitled "Conditional Uses" General Industrial (M-2) District, is hereby amended to read as follows:

"In the M-2 zone, the following uses may be permitted subject to approval of a conditional use permit:

A. Airports, heliports and landing strips.

B. Animal, food or beverage processing of the following kinds:

Breweries, distilleries and wineries.
Meat or fish products packing, canning or processing.
Vinegar, yeast and sauerkraut.

C. Asphalt, concrete and earth products activities of the following kinds:

Asphalt batching plants.
Concrete mixing and batching plants.
Rock crushing plants and aggregate dryers.
Sandblasting plants.
Butane service and filling stations.

D. Commercial and service type uses which the commission, after study and deliberation, finds are needed to serve the M-2 district, and which will not interfere with the orderly development of the industrial area, and which will be compatible with industrial uses.

E. Distilling of:

Alcohol.
Bones.
Coal.
Coal tar.
Coke.
Wood.
Heavy metal works of the following kinds:
Blast furnaces.
Boiler works.
Drop forge industries.
Drop hammers.
Forges, foundries and forging works.
Metal and metal ore reduction or smelting.
Rolling mills.

F. Manufacturing of:

Acetylene.
Ammonia.
Aniline dyes.
Asphalt or asphalt products.
Bleaching powder.
Bronze, babbitt metal and similar alloys.
Carbide.
Carbolic, hydrochloric, picric and sulfuric acid.
Caustic soda.
Cellophane.
Cellulose and celluloid.
Cement, lime, gypsum or plaster of Paris.
Charcoal, lampblack or fuel briquettes.
Chlorine.
Coal, coke or coal tar products.
Creosote.
Exterminating agents.
Fertilizer.
Film.

Gas.
Lacquer, shellac, turpentine, varnish or calcimine (kalsomine).
Linoleum or oilcloth.
Matches.
Nitrating of cotton and other materials.
Phenol.
Potash.
Pyroxylin.
Rubber (natural or synthetic).
Soap, tallow, grease and lard.
Radio transmitter towers, higher than fifty feet (50') above ground level.

G. Refining of:

Fats and oils.
Metals and metal ores.
Petroleum and petroleum products.
Sugar.
Salvage, wrecking and disposal activities of the following kind:
Automobile wrecking and salvage.
Building wrecking and salvage.
Dumps, including garbage and trash disposal.
Industrial waste material salvage, waste metal, rag, clothing, glass and paper salvage operations.
Sewer farm or sewage disposal plants.

H. Storage of:

Automobiles and other vehicles purchased for wrecking operations.
Fertilizer or manure.
House movers' equipment and buildings moved from other locations.
Oil or gas in amounts of two thousand five hundred (2,500) barrels or more.
Oil or gas within three hundred feet (300') of any residential zone, school or park.
Sand, gravel, rock or decomposed granite in amounts of two thousand (2,000) tons or more.
Used building materials or secondhand buildings."

SECTION 10. Chapter 18.156 of the Redlands Municipal Code, entitled "Development Provisions for Specific Uses," Article XII entitled "Warehouses and Logistics Distribution Centers," is hereby amended as follows:

"ARTICLE XII. Warehouses and Logistics Distribution Centers

18.156.900: DEFINITIONS:

ALTERATION:	Any construction or renovation to an existing structure other than repair or addition. A change, addition or modification in construction, change in occupancy or use, or structural repair to an existing building or facility. Alterations include, but are not limited to, remodeling, renovation, rehabilitation, reconstruction, historic restoration, resurfacing of interior circulation paths or vehicular ways, changes or rearrangement of the structural parts or elements, and changes or rearrangement in the plan configuration of walls and full-height partitions. Normal maintenance, reroofing, painting or wallpapering, or changes to mechanical and electrical systems are not alterations unless they affect the usability of the building or facility.
REPAIR:	*Repair* has the same meaning as defined in the California Building Code (Chapter 2, as amended, California Building Code).
WAREHOUSE:	Warehouse/distribution facilities primarily used for the storage and/or consolidation of manufactured goods before their distribution to retail locations or other warehouses. Warehouse/distribution centers are fifty thousand (50,000) square-feet or more in gross floor area or contain six (6) or more truck docks or dock high loading doors. They are characterized by dock high loading doors and could be on opposing sides of the building (cross dock facility); may include grade-level loading doors; interior clear heights a minimum of 28 to 36 feet to ceiling for the warehousing floor area; significant movement and storage of products, materials, or equipment; may include receiving, sorting, re-packaging, and/or re-distribution; truck activities frequently outside of the peak hour of the adjacent street system; and need freeway access. This definition excludes facilities owned and operated by a government agency or any public or private utilities. Warehousing and distribution facilities include, but are not limited to, the following types of uses: A. Warehousing distribution/high cube distribution centers. B. Parcel delivery terminals or truck terminals. C. Parcel sorting and distribution facilities. D. Package allocation for delivery drivers or independent delivery contractors. E. Parcel hub or high cube fulfillment center. F. Freight yards or forwarding terminals. G. Moving agencies. H. Shipping/receiving yards.
WAREHOUSING, ANCILLARY:	The use of a portion of a building for the related storage of goods of any type by one or two businesses and used for the sale or distribution of those goods directly to their customers. A manufacturing, assembly, service commercial, or other type of commercial or industrial use (i.e., primary use) manufactures

	and/or stores and distributes the goods or components that are produced or contained on-site, and therefore includes the related storage of those goods or items. Ancillary storage or warehousing is subordinate and incidental to the primary land use (e.g., manufacturing, assembly, service commercial, or other type of primary commercial or industrial use). Ancillary storage or warehousing may include ground level loading doors on one or more sides of the building, or not more than five (5) dock high loading doors on one side of the building only.

18.156.910: APPLICABILITY:

The provisions of this section shall apply to the following types of development projects:

A. New warehouse development projects that meet one of the following criteria (note: excludes government agency facilities and public or private utility facilities).

1. Gross floor area of fifty thousand (50,000) square-feet or more; or,
2. A structure with six (6) or more truck docks or dock high loading doors (does not include grade-level loading doors or loading spaces).

B. Required Compliance. No new warehouse development project shall be constructed, no redevelopment or reconstruction of a property for warehouse use, and no existing warehouse shall be moved, altered, or enlarged, except in accordance with the applicable development standards of this Article and/or applicable State law. If any provisions of this article conflict or are inconsistent with applicable State law, then State law shall prevail.

C. A property with a valid unexpired land use entitlement for a new warehouse or logistics distribution facility that has not yet been constructed or established as of the effective date of Ordinance No. 3002 shall have the same land use rights as if the structure had been existing on the effective date of Ordinance No. 3002.

18.156.920: SITE LOCATION REQUIREMENT:

A. No warehouses shall be located on a project site more than one mile (5,280 feet) from a freeway entrance/exit ramp to the Interstate Freeway System (Interstate 10 and Interstate 210). For purposes of this requirement, the linear distance shall be measured as a radius from a freeway ramp to any part of the subject property.

B. Assemblage of Parcels Prohibited: No warehouse development project, or redevelopment or reconstruction of a property for warehouse use, may assemble or merge additional properties for the purpose of developing, enlarging, expanding, or intensifying the use of an existing warehouse or logistics distribution facility.

18.156.930: SCREENING AND BUFFERING REQUIREMENTS:

A. Warehouse developments shall provide a solid decorative wall(s) of at least ten feet (10') in height when abutting any of the following land uses: any residence including private homes, condominiums, apartments, and living quarters; schools and preschools; daycare centers and in-home daycares; hospitals; long-term care facilities; retirement and nursing homes; community centers; places of worship; parks (excluding trails); and dormitories. The exterior treatment of the wall(s) shall be decorative or painted.

B. Unless physically impossible, loading docks and truck entries shall be oriented away from abutting sensitive receptors. To the greatest extent feasible, loading docks, truck entries, and truck drive aisles shall be located away from nearby sensitive receptors. In making feasibility decisions, the City must comply with existing laws and regulations and balance public safety and the site development's potential impacts to nearby sensitive receptors. Therefore, loading docks, truck entries, and drive aisles may be located nearby sensitive receptors at the discretion of the Planning Commission, but any such site design shall include measures designed to minimize overall impacts to nearby sensitive receptors.

C. Trees shall be used as part of the solid screen buffering treatment for any adjacent residential properties or properties with sensitive receptors. Trees used for this purpose shall be evergreen, drought-tolerant, minimum 36-inch box size, and shall be spaced no greater than 40-feet on center. Palm trees shall not be used for screening purposes. The property owner and any successors in interest shall maintain these trees for the duration of ownership ensuring any unhealthy or dead trees are replaced timely as needed.

D. Trees shall be installed in automobile (passenger vehicle) parking areas to provide at least thirty five percent (35%) shade cover of parking areas within fifteen (15) years. This requirement is in addition to the applicable standard design requirements for parking lot landscape and related improvements. Trees shall be planted that are capable of implementing this requirement.

18.156.940: TRAFFIC PATTERNS AND SIGN REQUIREMENTS:

A. Applicants for entitlements shall prepare and submit a Truck Routing Plan demonstrating the most direct route(s) to and from the Interstate Freeway System based on the city's latest Truck Route Map. Routes to or from freeway ramps shall not pass through any residential zones or districts.

B. A traffic impact assessment (TIA) report shall be prepared to evaluate a proposed warehouse project's compliance with the City's Measure U traffic system requirements, and shall include an evaluation of the City's streets and Truck Routes that provide vehicular access to the Interstate Freeway System, including, but not limited to: existing right-of-way width; roadway capacity to handle the proposed quantity of truck trips to be generated by the proposed use (including

any road widening that may be necessary); roadway design and improvements to handle the weight and frequency of proposed truck trips; intersection operations to freeway ramps and level of service analysis to include the proposed truck trips; truck turn radii at intersections; and other operational elements of the City's street network to serve the proposed use. The TIA may be prepared by a qualified consultant selected and directed by the City (and all consultant costs to be reimbursed by the applicant), or by a qualified traffic consultant selected by the applicant (and all work subject to the direction, review, and approval by the City).

C. Entry gates into the loading dock/truck court area with more than 20 loading docks shall be positioned after a minimum of 140 feet of total available stacking depth inside the property line (or alternatively, if 140 feet of depth is not feasible due to site constraints, then provide 70 feet of available stacking depth for two trucks side-by-side as an alternative design). The stacking distance shall be increased by 70 feet for every 20 loading docks beyond 50 docks. Queuing, or circling of vehicles, on public streets immediately pre- or post-entry to an industrial commerce facility is strictly prohibited unless queuing occurs in a deceleration lane or right turn lane exclusively serving the facility.

D. Prior to entitlement approval, applicants shall submit to the City, and obtain approval of, all turning templates to verify adequate truck turning movements at entrance and exit driveways as well as street intersections adjacent to industrial buildings. Unless not physically possible, truck entries shall be located on Collector streets or streets of a higher commercial classification, and vehicle entries shall be designed to prevent truck access on streets that are not Collector Streets (or streets of a higher commercial classification), including but not limited to by limiting the width of vehicle entries.

E. Anti-idling signs indicating a five (5) minute restriction on engine idling for diesel trucks shall be posted at warehouses and industrial commerce facilities along entrances to the site and within the dock areas and shall be strictly enforced by the facility operator (13 CCR § 2480).

F. Signs shall be installed at all truck exit driveways directing truck drivers to the truck route as indicated in the Truck Routing Plan to be routed to the Interstate Freeway System.

G. Signs and drive aisle pavement markings shall clearly identify the onsite circulation pattern to minimize unnecessary on-site vehicular travel.

H. Facility operators shall post signs in prominent locations inside and outside of the building indicating that off-site parking for any Medium Heavy-Duty trucks, Heavy Heavy-Duty trucks, truck trailers or cabs, and other operations-related vehicles is strictly prohibited. City may require facility operator to post signs on adjacent and nearby surface or residential streets indicating that off-site truck parking is prohibited by City ordinance.

I. All signs under this Section shall be legible, durable, and weather-proof.

18.156.950: SUSTAINABLE ENERGY:

A. A minimum of ninety percent (90%) of the on-site motorized operational equipment shall be zero emission (ZE).

B. All warehouse building roofs shall install photovoltaic (PV) solar collector system or other form of on-site renewable energy, provided such renewable energy source is recognized by the State of California as a renewable resource under the Renewable Portfolio Standard Program. The renewable energy system shall be metered separately from the nonrenewable metered power usage of the building (if not in conflict with other applicable regulations). The renewable energy system shall be built to generate an amount of electricity sufficient to meet the following criteria:

1. Annualized building demand based on the approved use or, if no use is proposed, then the demand for the most energy intensive use that could occupy the building; and

2. Annualized demand required to charge fully electric vehicles and trucks, assuming that all vehicles and trucks to the site are fully electric; and

3. A reasonable rate of efficiency loss over ten years.

Note: Electricity demand that exceeds the generation capacity of the on-site renewable energy system may be obtained from off-site energy sources or suppliers.

C. The warehouse building's rooftop that is not covered with solar panels or other utilities shall be constructed with light colored roofing material with a solar reflective index (SRI) in accordance with current California Energy Code regulations. This material shall be the minimum solar reflective rating of the roof material for the life of the building.

D. The on-site passenger vehicle parking shall include electric vehicle (EV) ready parking spaces in accordance with current requirements of the California Building Code, and at least fifty percent (50%) of the required EV parking spaces shall be equipped with working Level 2 Quick Charge EV charging stations installed and operational, prior to building occupancy. Signage shall be installed indicating EV charging stations and specifying that spaces are reserved for clean air/EV vehicles. Unless superior technology is developed that would replace the EV charging units, facility operator and any successors in interest shall be responsible for maintaining the EV charging stations in working order for the life of the facility.

E. Unless the owner of the facility records a covenant on the title of the underlying property ensuring that the property cannot be used to provide chilled, cooled, or freezer warehouse space, a conduit shall be installed during construction of the building shell from the electrical room to all (100%) of the loading dock doors that have potential to serve the refrigerated space. When tenant improvement building permits are issued for any refrigerated warehouse space, electric plug-in units shall be installed at every dock door servicing the refrigerated space to allow transport refrigeration units (TRUs) to plug in. Truck operators with TRUs shall be required to utilize electric plug-in units when at loading docks.

18.156.960: OPERATION AND CONSTRUCTION:

A. Cool surface treatments shall be added to all drive aisles and parking areas, or such areas shall be constructed with a solar-reflective cool pavement such as concrete. Solar collectors may be installed on support structures that provide shade over parking areas to achieve minimum requirements.

B. To ensure that warehouse electrical rooms are sufficiently sized to accommodate the potential need for additional electrical panels, either a secondary electrical room shall be provided in the building, or the primary electrical room shall be sized twenty-five percent (25%) larger than is required to satisfy the service requirements of the building or the electrical gear shall be installed with the initial construction with 25% excess demand capacity.

C. All exterior light fixtures (including but not limited to parking lot lighting, wall fixtures, roof fixtures, light poles, etc.) visible from public right-of-way or abutting properties shall have shielding affixed to contain illumination within the subject property and prevent light trespass and glare overspill.

D. The facility operator shall be required to perform regular maintenance of building structures, landscaping, and paved surfaces to ensure good physical condition and appearance.

E. For any sites with warehouses that are abutting or adjacent to any residential properties or properties containing sensitive receptors, any outdoor storage of materials, high-pile storage, or any other manner of storage or staging shall not exceed the height of the perimeter wall.

F. Additional operating conditions may be enacted for an individual Warehouse project pursuant to a Conditional Use Permit (Redlands Municipal Code Chapter 18.192) for the purpose of avoiding or reducing potential off-site nuisance effects of the warehouse facility (including but not limited to traffic, parking, noise, vibration, air quality emissions, etc.) on nearby sensitive receptors or residential districts, or to protect the public health, safety, or general welfare."

SECTION 11. Redlands Municipal Code Chapter 18.156, Article XII entitled "Warehouses and Logistics Distribution Centers," is hereby amended to add Section 18.156.970 as follows:

"18.156.970: REBUILDING PROVISIONS FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION CENTERS:

A. For warehouses and logistics distribution facilities existing as of the effective date of Ordinance No. 3002, the criteria for alterations or repairs to the existing structure or property are as follows:

1. Ordinary repair and maintenance may be performed on a structure or property subject to the provisions of this article, and in accordance with applicable law (e.g., California Building Code, California Fire Code, etc.).

2. Improvements to the existing structure including technology upgrades (e.g., seismic strengthening, energy use efficiency, PV solar or re-roof, water use efficiency, reductions to greenhouse gas emissions, hazardous materials remediation, etc.) may be installed on a structure or property subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

3. Warehouses and logistics distribution facility buildings may be voluntarily rebuilt, reconstructed, or otherwise altered, subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

4. If the warehouse or logistics distribution facility building is involuntarily damaged or destroyed by natural disasters (i.e., fire, flood, earthquake or other calamity or acts of God), the entirety of the structure may be rebuilt subject to the provisions of this article, and in accordance with applicable laws (e.g., California Building Code, California Fire Code, etc.).

B. Existing warehouses and logistics distribution facilities (existing as of the effective date of Ordinance No. 3002) may be rebuilt to the previously existing square-footage (building footprint), previously existing height, and previously existing number of truck docks if the subject property meets the following criteria:

1. The warehouse or logistics distribution use was legally established prior to the effective date of Ordinance No. 3002; or if not yet established, the subject property had a valid land use entitlement issued prior to the effective date of Ordinance No. 3002.

2. The Development Services Director has determined the existing business to be a permitted or conditionally permitted use.

3. An applicable building permit(s) shall be obtained for reconstruction, if required.

4. A change in ownership or tenancy without any change in use or occupancy shall not affect any of the rebuilding rights, privileges, and responsibilities provided pursuant to this section.

5. It shall be the property owner's responsibility to provide evidence or information to justify the establishment of rebuilding rights.

C. Existing warehouses and logistics distribution facilities (existing as of the effective date of Ordinance No. 3002) may be altered and request an increase to the building height pursuant to the following criteria:

1. Building height may be increased up to the maximum height allowable within the applicable land use district (or 50 feet if no maximum is specified) to incorporate technology upgrades, energy efficiency improvements, or other justifiable economic or environmental reasons; and/or may increase the number of previously existing truck dock positions; provided the structure meets the criteria listed below.

a. The subject property meets all applicable criteria in Section 18.156.970(B).

b. The subject property obtains a Conditional Use Permit issued pursuant to Chapter 18.192 of this title.

c. Construction or redevelopment of a building involving additional height shall include the feasible provisions of Section 18.156.930 through 18.156.960 of this article, as determined by the Planning Commission (the location requirements of Section 18.156.920(A) shall not apply). For purposes of this article, “feasible” has the same meaning as California Code of Regulations Title 14, § 15364.

d. Complete an environmental review process, if applicable, in accordance with the California Environmental Quality Act for a proposed project that will increase building height, increase the number of truck docks, or change non-refrigerated space to refrigerated space.

e. The applicant shall prepare and submit the following in conjunction with a development application for a land use entitlement:

i. Circulation studies, prepared by a traffic engineer, showing the movement of vehicular and truck traffic to and from the subject property, and to and from existing thoroughfares. Special engineering features and/or traffic regulation devices needed to facilitate or ensure safety of circulation may be required.

ii. A landscaping and tree planting plan, prepared by a landscape architect.

iii. An economic feasibility report or market analysis, prepared by a qualified economist, justifying the need to increase the building height and/or increase the number of truck docks.

iv. An energy audit analysis report to identify current (baseline) conditions for the existing structure; and an energy analysis for the proposed modified facility to demonstrate compliance with the California Building Code and that there will be a demonstrated improvement to energy efficiency.”

SECTION 12. Severability. If any section, subsection, subdivision, sentence, clause, phrase, or portion of this Ordinance for any reason is held to be invalid or unconstitutional by the decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this Ordinance. The City Council hereby declares that it would have adopted this Ordinance, and each section, subsection, subdivision, sentence, clause, phrase, or portion thereof, irrespective of the fact that any one or more sections, subsections, subdivisions, sentences, clauses, phrases, or portions thereof be declared invalid or unconstitutional.

SECTION 13. The Mayor shall sign this ordinance and the City Clerk shall certify to the adoption of this ordinance and shall cause it, or a summary of it, to be published once in a newspaper of general circulation within the City, and thereafter, this ordinance shall take effect as provided by law.

ADOPTED, SIGNED AND APPROVED this ___ day of _____, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk, City of Redlands, hereby certify that the foregoing Ordinance was duly adopted by the City Council at the regular meeting thereof, held on the _____ day of _____, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

RESOLUTION NO. 8793

A RESOLUTION OF THE CITY OF REDLANDS AMENDING NON-RESIDENTIAL SPECIFIC PLANS AND CONCEPT PLANS TO PROHIBIT NEW WAREHOUSES AND LOGISTICS DISTRIBUTION USES, AS DEFINED, IN ALL COMMERCIAL AND INDUSTRIAL DISTRICTS OF SPECIFIC PLANS, WHILE ALLOWING FOR EXISTING WAREHOUSES AND LOGISTICS DISTRIBUTION USES TO REMAIN AS PERMITTED OR CONDITIONALLY PERMITTED USES SUBJECT TO NEW REBUILD PROVISIONS CONTAINED IN REDLANDS MUNICIPAL CODE TITLE 18.

WHEREAS, the City Council of the City of Redlands has initiated Ordinance Text Amendment No. 372, in accordance with Chapter 18.204 (Amendments) of the Redlands Municipal Code, as the public necessity, convenience, or general welfare justifies such action; and

WHEREAS, over the past twenty years, Redlands has experienced the construction of numerous large warehouses and logistics distribution facilities in and around the City of Redlands including the unincorporated County jurisdiction located in northwest Redlands; and

WHEREAS, on September 29, 2024, the Governor of the State of California signed Assembly Bill (AB) 98 to add Section 65302.02 to, and to add Chapter 2.8 (commencing with Section 65098) to Division 1 of Title 7 of, the Government Code, and to add Sections 40458.5 and 40522.7 to the Health and Safety Code, relating to land use, and the "Warehouse Concentration Region" defined therein includes the City of Redlands among other nearby cities and counties; and

WHEREAS, two major transportation corridors (Interstate 10 and Interstate/S.R. 210 freeways) serve the Southern California region and are gateways to the Interstate Highway System, and both freeways pass through the City of Redlands, which contributes to a significant quantity of heavy-truck and other vehicular traffic to pass through the City to reach destinations located outside the City of Redlands as well as within the unincorporated "donut hole" area; and

WHEREAS, heavy-truck traffic that serves several million square feet of warehousing and logistics distribution uses located within the unincorporated County island area (surrounded by the City of Redlands) must pass through the City and utilize City streets on a daily basis at all hours of the day and night; and

WHEREAS, the residents and visitors of the City of Redlands may experience exposure to environmental effects (such as numbers of truck trips, vehicle miles traveled, greenhouse gas emissions affecting air quality, vehicular noise, etc.) and other externalities from such warehousing and logistics distribution uses; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about March 24, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on April 14, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, on or about April 21, 2026, the Secretary to the Planning Commission gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which Ordinance Text Amendment No. 372 would be considered by the Planning Commission; and

WHEREAS, on May 12, 2026, the Planning Commission held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, Ordinance Text Amendment No. 372 and related Specific Plan Amendments; and

WHEREAS, following the public hearing on May 12, 2026, the Planning Commission determined that Ordinance Text Amendment No. 372 would be in conformity with the 2035 General Plan, and would be consistent with goals of the General Plan for transportation, connectivity, compatibility and harmonious relationship of different land uses; and

WHEREAS, on May 12, 2026, the Planning Commission recommended to the City Council that the proposed Specific Plan Amendment(s) be approved; and

WHEREAS, this Resolution is exempt from environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines; and

WHEREAS, in accordance with Government Code § 65854 and/or § 65090, the City Clerk gave notice by publication in a newspaper of general circulation of the holding of a public hearing at which the proposed Resolution would be considered by City Council; and

WHEREAS, on June 16, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, the proposed Specific Plan Amendments and continued the public hearing; and

WHEREAS, on September 1, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, the proposed Specific Plan Amendments and continued the public hearing to October 6, 2026; and

WHEREAS, on October 6, 2026, the City Council held a noticed public hearing at which interested persons had an opportunity to testify in support of, or opposition to, the proposed Specific Plan Amendments.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF REDLANDS RESOLVES AS FOLLOWS:

SECTION 1. Environmental Determination. The proposed Specific Plan Amendments do not require environmental review in accordance with Sections 15061(b)(3), 15308, and 15378(b)(5) of the California Environmental Quality Act Guidelines. Pursuant to Section

15378(b)(5) of the California Environmental Quality Act ("CEQA"), this proposal is an organizational or administrative activity of the City that will not result in direct or indirect physical changes in the environment, and therefore not a project. Additionally, pursuant to CEQA Guidelines Section 15061(b)(3), this proposal is exempt from CEQA review because there is no possibility that the specific plan amendment(s) may have a significant effect on the environment, insofar as it would amend the lists of permitted land uses in the City of Redlands. Furthermore, even if the proposal is considered a project, the proposed specific plan amendment(s) is categorically exempt under CEQA Guidelines Section 15308, because it is clear that it will not create an environmental impact and the action will assure the maintenance, enhancement, or protection of the environment through the adoption of regulations prohibiting new large warehouses and logistics distribution facilities. Accordingly, no further environmental review is necessary.

SECTION 2. Concept Plan No. 1 (CP-1), Section III entitled "Development Standards," subsection 'B' entitled "Commercial Industrial District," Part 1 entitled "Permitted Uses" thereof, is hereby amended as follows:

"g. Other uses typically associated with light manufacturing within enclosed buildings, including but not limited to the following:

- Business, technical, trade or professional schools
- Clubs, lodges and similar organizations
- Government buildings
- Warehouses, not to exceed 50,000 square feet in any single building
- Wholesale trade of most consumer items including drugs, dry goods, apparel, groceries, building materials and paper products.
- Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code."

SECTION 3. Concept Plan No. 1 (CP-1), Section III entitled "Development Standards," subsection 'B' entitled "Commercial Industrial District," Part 2 entitled "Conditionally Permitted Uses" thereof, is hereby amended as follows:

"d. Large Warehouse-Distribution Buildings.
Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code."

SECTION 4. Concept Plan No. 2 (CP-2), Section 3.2 entitled "Regional Industrial District," subsection 'A' entitled "Permitted Uses," Part 3 thereof is hereby amended as follows:

"3. Wholesale trade:

Wholesale trade of durable and non-durable goods to commercial, industrial and professional business uses, including motor vehicles, sporting goods, electrical appliances, hardware, machinery and equipment for industry, construction, professional and service establishments.

Warehouses and logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code."

SECTION 5. Specific Plan No. 40 (East Valley Corridor Specific Plan), Chapter 9 titled "Commercial Industrial District," Section EV3.0910 (Permitted Land Uses), part 7, is hereby amended as follows:

"(7) Other uses typically associated with light manufacturing within enclosed buildings, including but not limited to the following:

- Business, technical, trade, or professional schools
- Clubs, lodges, and similar organizations
- Government buildings
- Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, that were legally established prior to the effective date of Ordinance No. 3002 (or the property has a valid land use entitlement approved prior to the effective date of Ordinance No. 3002). Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code.
- Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors (see Chapter 18.156, Article XII, of Redlands Municipal Code Title 18).
- Warehousing, ancillary to another primary use (see Chapter 18.156, Article XII, of Redlands Municipal Code Title 18).
- Wholesale trade of most consumer items, including motor vehicles, drugs, dry goods, apparel, groceries, building materials and paper products."

SECTION 6. Specific Plan No. 40 (East Valley Corridor Specific Plan), Chapter 10 titled "Regional Industrial," Section EV3.1010 (Permitted Land Uses), part 4, is hereby amended as follows:

"(4) Wholesale Trade, such as:

- Warehouses or logistics distribution with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, that were legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code.
- Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors (see Chapter 18.156, Article XII, of Redlands Municipal Code Title 18).
- Wholesale trade of durable and non-durable goods to commercial, industrial and professional uses, including motor vehicles, sporting goods, electrical appliances, hardware, machinery and equipment for industry, construction, professional and service establishments."

SECTION 7. Specific Plan No. 25 (East Valley Complex), Section 3 titled "Property Development Standards," subsection (B) titled "Office/Industrial," part 3 (Uses Prohibited) is hereby amended as follows:

"Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, are not permitted."

SECTION 8. Specific Plan No. 32 (Redlands Aviation Park), Section 3 titled "Property Development Standards," subsection (B) titled "Office/Industrial District," part 2 titled "Permitted Uses," subsection (c) is hereby amended as follows:

"Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, are not permitted."

SECTION 9. Specific Plan No. 33 (Centennial Commerce Park), Section 3 titled "Development Standards," subsection (B) titled "Office/Industrial," part 2 titled "Permitted Uses," subsection (c) is hereby amended as follows:

"Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, are not permitted."

SECTION 10. Specific Plan No. 42 (Redlands Research Park), Section 3 titled "Development Standards," subsection (A) titled "Office/Industrial Land Use," part 1 (Permitted Uses), is hereby amended as follows:

"1. Permitted Uses - No building, structure or land shall be used, and no building or structure shall be hereafter erected, structurally altered or enlarged except for the following purposes:

a. Offices, including but not limited to:

Accounting, auditing, and bookkeeping services
Administrative headquarters
Architectural, planning andengineering offices
Business associations
Corporate headquarters
Banks and finance companies
Insurance offices
Law offices
Real estate offices
Such other office uses as deemed similar to the above.

b. Research and development, including but not limited to:

Biochemical and Chemical
Metallurgical Pharmaceutical
Medical and dental
Film and photographic
Electrical and Mechanical
Optical

c. Manufacturing, including but not limited to:

Establishments primarily engaged in manufacturing the following products:

Apparel, drapery, upholstery,millinery, and related cloth and clothing
Furniture and fixtures, including office furniture, store fixtures, blinds and shades, and shelving
Paper products, including envelopes, bags, wallpaper, containers, pressed and molded pulp goods
Publishing, including newspapers, business forms, typesetting, photoengraving, bookbinding, and printing
Fabricated plastic products
Fabricated metal products
Professional and scientific goods, including measuring instruments, clocks and watches, optical goods, surgical and medical instruments, photographic equipment, engineering, computers, and similar equipment and

supplies
Miscellaneous manufactured goods, including jewelry, lapidary, precious metals, toys, sporting goods, musical instruments, and similar goods.

Warehouse and distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, that were legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code.

Warehousing, in buildings with less than 50,000 square-feet in gross floor area, and not more than five truck docks or dock high loading doors."

SECTION 11. The adopted Planned Development entitlements within the City of Redlands are hereby amended to prohibit the development or establishment of new warehouses and logistics distribution centers, as defined in Article XII of Chapter 18.156 of the Redlands Municipal Code, while allowing existing warehouses to remain as permitted or conditionally permitted uses within their respective Planned Development (PD) entitlements:

"Warehouses or logistics distribution centers with 50,000 square-feet in gross floor area or more, or having more than five truck docks or dock high loading doors, that were legally established prior to the effective date of Ordinance No. 3002. Such warehouses or logistics distribution facilities shall be subject to the applicable provisions contained in Chapter 18.156, Article XII, of the Redlands Municipal Code."

The applicable Planned Development entitlements are the following:

a. Planned Development No. 1 (PD 1);
b. Planned Development No. 3 (PD 3);
c. Planned Development No. 4 (PD 4);
d. Planned Development No. 7 (PD 7).

SECTION 12. If any section, subsection, subdivision, sentence, clause, phrase, or portion of this resolution for any reason is held to be invalid or unconstitutional by the decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this resolution. The City Council hereby declares that it would have adopted this resolution, each section, subsection, subdivision, sentence, clause, phrase, or portion thereof, irrespective of the fact that any one or more sections, subsections, subdivisions, sentences, clauses, phrases, or portions thereof be declared invalid or unconstitutional.

SECTION 13. Effective Date. This Resolution shall become effective on the effective date of Ordinance No. 3002.

ADOPTED, SIGNED AND APPROVED this ___ day of _____, 2026.

_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

I, Jeanne Donaldson, City Clerk, City of Redlands, hereby certify that the foregoing Resolution was duly adopted by the City Council at the regular meeting thereof, held on the ___ day of _____, 2026, by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Jeanne Donaldson, City Clerk

City Council **AGENDA ITEM NO. L1.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Approve the First Amendment to the Public Works Contract with B-81 Paving Inc. for On-Call Pavement Repair Services for Water Utilities to increase the not to exceed amount from $600,000 to $900,000 (Municipal Utilities and Engineering Director Heredia)

MOTION:

If the City Council determines that staff recommendation is appropriate, the following motion is provided:

I move to approve the First Amendment to the Public Works Contract with B-81 Paving, Inc., for On-Call Pavement Repair Services for Water Utilities to increase the not to exceed amount of $600,000 to $900,000.

RECOMMENDATION:

Staff recommends that the City Council approve the First Amendment to the Public Works Contract with B-81 Paving, Inc., for On-Call Pavement Repair Services for Water Utilities to increase the not to exceed amount of $600,000 to $900,000.

DISCUSSION:

The Municipal Utilities and Engineering Department (MUED) performs approximately 250 water utility repairs annually throughout the City's water service area, including repairs to water mains, service lines, valves, blow-offs, and other associated infrastructure. These repairs typically require the removal of existing asphalt concrete (AC) pavement and excavation of the roadway to access the affected utility facilities. After the utility repair, excavated areas are temporarily restored with aggregate base and cold-mix asphalt pending permanent pavement restoration with hot-mix asphalt (HMA). Historically, contractors have performed permanent pavement restoration on an as-needed basis through individual work requests issued by MUED staff.

On July 21, 2026, the City Council approved a Public Works Contract with B-81 Paving, Inc., in an amount not to exceed $600,000 for Fiscal Years 2026/27 and 2027/28 to provide permanent pavement restoration associated with water utility repairs throughout the City and determined the Project to be exempt from environmental review pursuant to Section 15301 of the State's Guidelines implementing the California Environmental Quality Act.

The Contract allows the Water Division to promptly restore roadway surfaces following emergency and routine water system repairs, including main line breaks, service line failures, valve and appurtenance repairs, and other utility-related excavations. Since the Contract was awarded, the Water Division has experienced an increased volume of water main and associated infrastructure repairs throughout the City's water service area, resulting in additional pavement restoration requirements beyond the level initially anticipated. In addition to addressing these recent repairs, the contract continues to be utilized to complete outstanding pavement restoration resulting from prior water infrastructure failures, utility improvements, and associated trenching activities.

Additional funding is therefore necessary to maintain continuity of pavement restoration services, minimize the duration of temporary roadway repairs, and ensure that disturbed roadway surfaces are restored in accordance with City standards. Based on current repair activity, anticipated ongoing water system maintenance needs, and the remaining Contract term, staff anticipates that the requested additional funding will provide sufficient capacity for the Water Division to address pavement restoration requirements through the end of the Contract period.

ALTERNATIVES:

The City Council may choose not to approve the First Amendment and provide alternative direction to staff.

STRATEGIC PLAN:

N/A

SUBMITTED BY:
Monica Heredia, Municipal Utilities and Engineering Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
Goutam K. Dobey, City Engineer
James Garland, Finance Director

PREPARED BY:
Paul Mariscal, Water Utility Manager

FISCAL IMPACT

Fiscal Year: FY 2026/27 and FY 2027/28

Revenue Generating: No

Budgeted Y/N: Yes

Account No.: 501900

Additional Appropriation Required: No

Discussion:

There is no additional fiscal impact associated with this action. Funding for these services is included in the FY2026/27 and FY 2027/28 Water Service Fund budgets.

Attachments

A_B-81_Paving_Inc_1st_Amendment.pdf
B_B-81_Executed_Contract_For_Reference_Only.pdf

FIRST AMENDMENT TO PUBLIC WORKS CONSTRUCTION CONTRACT

This first amendment ("First Amendment") to the Public Works Construction Contract for On-Call Pavement Repair Services for Water Utilities dated July 21, 2026 ("Contract"), by and between the City of Redlands, a municipal corporation and a general law city (hereinafter "City"), and B-81 Paving Inc, a California Corporation (hereinafter "Contractor"), is made and entered into this 6th day of October, 2026.

RECITALS

WHEREAS, it is the desire of the City and Contractor to amend their existing Contract, specifically to amend the contract sum, increasing the total not to exceed the contract amount to Nine Hundred Thousand dollars ($900,000).

NOW, THEREFORE, for good and valuable consideration in the receipt of which is hereby acknowledged, City and Contractor agree as follows:

AGREEMENT

Section 1. Contract Sum, as set forth in Section 2 of the Contract, is hereby amended to read as follows:

"**2. CONTRACT SUM:** City shall pay Contractor the sum not to exceed Four Hundred and Fifty Thousand dollars ($450,000.00) for fiscal year 2026/27; and the sum not to exceed Four Hundred and FiftyThousand dollars ($450,000.00) for fiscal year 2027/28; totaling an amount not to exceed Nine Hundred Thousand dollars ($900,000.00) as consideration for its performance of the Work in accordance with the terms and conditions set forth in the Contract Documents. Pursuant to Public Contract Code Section 22300, Contractor has the option to deposit securities with an escrow agent as a substitute for retention of earnings required to be withheld by City pursuant to an escrow agreement as set forth in Public Contract Code section 22300."

Section 2. All other provisions of the Agreement shall remain unchanged by this First Amendment and in effect.

IN WITNESS WHEREOF, the parties have executed this First Amendment, to be effective as of the 6th day of October, 2026.

CITY OF REDLANDS

_____
Mario Saucedo, Mayor

B-81 PAVING INC

By: _____
Adalberto Bedolla, President

ATTEST:

_____
Jeanne Donaldson, City Clerk

PUBLIC WORK CONSTRUCTION CONTRACT

This Public Work Construction contract ("Contract") is made and entered into this 21st day of July, 2026, by and between the City of Redlands, a municipal corporation, organized and existing under the laws of the State of California (hereinafter "City"), and B-81 Paving Inc (hereinafter "Contractor"). City and Contractor are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

In consideration of the mutual promises contained herein, City and Contractor agree as follows:

1. **SCOPE OF WORK:** Contractor shall furnish all materials and will perform all of the work for the following: On-Call Pavement Repair Services for Water Utilities, complete all items as required by the Contract Documents (as herein defined) and Specifications for City's On-Call Pavement Repair Services for Water Utilities (the "Work").

2. **CONTRACT SUM:** City shall pay Contractor the sum not-to-exceed Three Hundred Thousand dollars ($300,000.00) for fiscal year 2026/27; and the sum not to exceed Three Hundred Thousand dollars ($300,000.00) for fiscal year 2027/28; totaling an amount not to exceed Six Hundred Thousand dollars ($600,000.00) as consideration for its performance of the Work in accordance with the terms and conditions set forth in the Contract Documents. Pursuant to Public Contract Code Section 22300, Contractor has the option to deposit securities with an escrow agent as a substitute for retention of earnings required to be withheld by City pursuant to an escrow agreement as set forth in Public Contract Code section 22300.

3. **TIME FOR COMPLETION:** The Work shall be completed within seven hundred (700) calendar days from and after the date of City's issuance of a Notice to Proceed to Contractor.

4. **LIQUIDATED DAMAGES:** Contractor's failure to complete the Work within the time allowed will result in damages being sustained by City. Such damages are, and will continue to be, impracticable and extremely difficult to determine. Accordingly, Contractor shall pay to City, or have withheld from monies due to Contractor, the sum of Five Hundred dollars ($500.00) for each consecutive calendar day in excess of the specified time for completion of the Work. Execution of this Contract shall constitute agreement by City and Contractor that Five Hundred dollars ($500.00) per day is the estimated damage to City caused by the failure of Contractor to complete the work within the allowed time. Such sum is liquidated damages and shall not be construed as a penalty, and may be deducted from payments due Contractor if such delay occurs.

5. **CONTRACT DOCUMENTS:** This Contract incorporates by reference the following: Notice Inviting Bids, Instructions to Bidders, Contractor's Proposal, Bid Bond, Agreement, Performance Bond, Labor and Material Bond, Plans, General Conditions, Special Provisions and Specifications, and any addenda thereto (collectively, the "Contract Documents").

6. **ATTORNEYS' FEES:** In the event any action is commenced to enforce or interpret the terms or conditions of this Contract, or the Contract Documents, the prevailing Party in such action, in addition to any costs and other relief, shall be entitled to recover its reasonable attorneys' fees, including fees for use of in-house counsel by a Party.

7. **RESOLUTION OF CONSTRUCTION CLAIMS:** Claims by Contractor in the amount of Three Hundred Seventy-Five Thousand dollars ($375,000.00) or less shall be made by Contractor and processed by the City pursuant to the provisions of Part 3, Chapter 1, Article 1.5 of the Public

Contract Code (commencing with Section 20104). All claims shall be in writing and include the documents necessary to substantiate the claim. Nothing in subdivision (a) of Public Contract Code Section 20104.2 shall extend the time limit or supersede the notice requirements provided in this case from filing claims by Contractor.

8. **ELIGIBILITY OF CONTRACTOR/SUBCONTRACTOR:** Contractor and all of its subcontractors shall abide by California Public Contract Code, Section 6109, and California Labor Code Sections 1777.1 and/or 1777.7, and certify that they are not debarred and are eligible to work on this project.

9. **ASSIGNMENT OF AGREEMENT:** No assignment by a Party of any rights or interests under this Contract shall be binding on another Party without the written consent of the Party sought to be bound.

10. **SUCCESSORS AND ASSIGNS:** City and Contractor each binds itself and their respective successors and assigns in respect to all covenants, agreements, and obligations contained in the Contract Documents.

11. **SEVERABILITY:** Any provision or part of the Contract Documents held to be void or unenforceable under any law or regulation shall be deemed stricken, and all remaining provisions shall continue to be valid and binding upon City and Contractor.

IN WITNESS WHEREOF, the Parties hereto have executed this Contract the day and year first written above.

CITY OF REDLANDS

(SEAL)

By: _____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

(SEAL)

B-81 Paving, Inc.
Name of Contractor

By: _____
Signature of Authorized Agent

President
Title

_____
Signature of Authorized Agent (if necessary)

_____
Title

1026076
Contractor's License No.

City Council **AGENDA ITEM NO. L2.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Consideration of an agreement with Three Peaks Corp. for the crushing of concrete stockpile for a three-year term in a total amount not to exceed $300,000 and determination that the project is exempt from environmental review pursuant to Section 15301 of the State's Guidelines implementing the California Environmental Quality Act (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move to determine that approval of the agreement with Three Peaks Corp. for crushing of concrete stockpile at the California Street Landfill is categorically exempt from environmental review pursuant to Section 15301 of the state's Guidelines implementing the California Environmental Quality Act; and

2. I move to approve an agreement with Three Peaks Corp. for crushing the concrete stockpile at the California Street Landfill for a three-year term in a total amount not to exceed $300,000.

RECOMMENDATION:

Staff recommends that City Council determine that approval of the agreement with Three Peaks Corp. for crushing of concrete stockpile at the California Street Landfill is categorically exempt from environmental review in accordance with California Environmental Quality Act Guidelines Section 15301. Staff further recommends that the City Council approve an agreement with Three Peaks Corp. for crushing the concrete stockpile at the California Street Landfill for a three-year term in a total amount not to exceed $300,000.

DISCUSSION:

The City of Redlands Facilities and Community Services Department Solid Waste Division manages the daily operations at the California Street Landfill located at 2151 Nevada Street. The landfill receives material from residential and commercial customers for various construction activities throughout the City that generate concrete waste. Landfill operations include segregating, processing, crushing, and the stockpiling of concrete for the purpose of diverting concrete debris from the City’s landfill. This process conserves landfill air space and provides recycled material for the use as an aggregate base for onsite improvements performed by City staff. In addition, the crushing and diversion of this material is a regulatory requirement of CalRecycle. Crushing services are performed periodically as stockpiles accumulate to a level that makes processing operationally efficient.

In accordance with the City's procurement policy, staff issued a Request for Bid (RFB) for as-needed crushing of concrete stockpiles at the California Street Landfill. On June 23, 2026, the City Clerk's office received and opened two (2) bids. Staff evaluated the bids for conformance with the RFB specifications and the City's purchasing requirements. Three Peaks Corp. met all bidding requirements and purchasing guidelines and was deemed the lowest responsive and responsible bidder.

Staff recommends that the City Council approve an agreement with Three Peaks Corp. for a three-year term and a total amount not to exceed $300,000. The RFB was structured on an as-needed basis and the quantities included in the price sheet are not guaranteed quantities. The $95,300 bid reflects unit pricing for an anticipated crushing operation. Actual work will be ordered on an as-needed basis depending upon the quantity of accumulated material during the three-year contract term. Accordingly, the proposed agreement establishes a total not to exceed amount of $300,000 to accommodate the City's anticipated as-needed crushing services over the three-year term.

VENDOR NAME	BID AMOUNT
Three Peaks Corp.	$95,300
American International Environmental Inc.	$98,795

The proposed project is categorically exempt from the requirements of the California Environmental Quality Act's guidelines pursuant to Section 15301. The section pertains to the normal operations of existing facilities, and the proposed project is consistent with this exemption as the proposed activity does not increase the existing operational capacity or expand the use of the landfill facilities.

ALTERNATIVES:

The City Council may choose not to enter into the proposed agreement; however, that may result in the inability to eliminate the stockpile of accumulated concrete debris and place the city in violation of the California Street Landfill's operating permit.

STRATEGIC PLAN:

Supports Priority D- Sustainability.

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
Dana Abramovitz-Daniel, Procurement Manager
James Garland, Finance Director

PREPARED BY:
Nathalie Ayala, Administrative Assistant

FISCAL IMPACT

Fiscal Year: FY 2026-27

Revenue Generating: No

Amount: $300,000

Budgeted Y/N: Y

Account No.: 511900-6710

Additional Appropriation Required: No

Discussion: Sufficient funding for this agreement is included in the Solid Waste Division's budget for Fiscal Year 2026-27 as approved by the City Council.

Attachments

Agreement_w_Three_Peaks_Corp.pdf

BID_Report_-_As-Needed_Crushing_of_Concrete_Stockpile.pdf

AGREEMENT TO PERFORM NON-PROFESSIONAL SERVICES FOR IMPROVEMENT TO PUBLIC BUILDINGS AND GROUNDS

This agreement for the provision of as-needed crushing of concrete stockpile at the California Street Landfill ("Agreement") is made and entered in this 6th day of October, 2026 ("Effective Date"), by and between the City of Redlands, a municipal corporation ("City") and Three Peaks Corp., a California corporation ("Contractor"). City and Contractor are sometimes individually referred to herein as a "Party" and, together, as the "Parties." In consideration of the mutual promises contained herein, City and Contractor agree as follows:

ARTICLE 1 – ENGAGEMENT OF CONTRACTOR

1.1 City hereby engages Contractor to perform as-needed crushing of concrete stockpile at the California Street Landfill services for City (the "Services"). The Services that Contractor shall perform are more particularly described in Exhibit "A," titled "Scope of Services," which is attached hereto and incorporated herein by this reference.

1.2 The Services shall be performed by Contractor in a professional manner, and Contractor represents that it has the skill and the professional expertise necessary to provide the Services to City at a level of competency presently maintained by other practicing professional Contractors in the industry providing like and similar types of Services.

ARTICLE 2 – RESPONSIBILITIES OF CONTRACTOR

2.1 Contractor shall comply with all applicable federal, state and local laws and regulations in the performance of the Services including, but not limited, to all applicable Labor Code and prevailing wage laws and non-discrimination laws, including the Americans with Disabilities Act. Pursuant to Labor Code section 1773.2, copies of the prevailing rates of per diem wages as determined by the Director of the California Department of Industrial Relations for each craft, classification or type of worker needed to undertake the Services are on file at City's Municipal Utilities and Engineering Department, located at the Civic Center, 35 Cajon Street, Suite 15A (Mailing: P.O. Box 3005), Redlands, California 92373.

2.2 Contractor acknowledges that if it violates the Labor Code provisions relating to prevailing wages that City may enforce such provisions by withholding payments to Contractor or its subcontractors pursuant to Labor Code section 1771.6.

2.3 If Contractor executes an agreement with a subcontractor to perform any portion of the Services, Contractor shall comply with Labor Code sections 1775 and 1777.7, and shall provide the subcontractor with copies of the provisions of Labor Code sections 1771, 1775, 1776, 1777.5, 1813 and 1815. Contractor acknowledges that the statutory provisions establishing penalties for failure to comply with state wage and hour laws and to pay prevailing wages may be enforced by City pursuant to Labor Code sections 1775 and 1813.

2.4 Contractor and its subcontractors shall comply with the provisions of Labor Code section 1776 regarding payroll records maintenance, certifications, retention and inspection.

2.5 Contractor acknowledges that eight (8) hours constitutes a legal day's work pursuant to Labor Code section 1810.

2.6 Contractor shall comply with the provisions of Labor Code section 1777.5 as to apprenticeships, and Labor Code sections 1771, 1775, 1776, 1777.5, 1813 and 1815.

2.7 Pursuant to Public Contract Code section 7103.5(b), Contractor offers and agrees to assign to City all rights, title and interest in and to all causes of action it may have under section 4 of the Clayton Act (15 U.S.C. section 15) or under the Cartwright Act (Chapter 2 (commencing with section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, goods or materials pursuant to this Agreement.

ARTICLE 3 – RESPONSIBILITIES OF CITY

3.1 City shall make available to Contractor information in its possession that may reasonably assist Contractor in performing the Services.

3.2 City designates Tabitha Crocker, Facilities and Community Services Director, as City's representative with respect to performance of the Services, and such person shall have the authority to transmit instructions, receive information, interpret and define City's policies and decisions with respect to performance of the Services.

ARTICLE 4 – PERFORMANCE OF SERVICES

4.1 The Services shall commence as of the Effective Date of this Agreement. Contractor shall perform and complete the Services in a prompt and diligent manner in accordance with the schedule set forth in Exhibit "A," which is attached hereto and incorporated herein by this reference.

4.2 The term of this Agreement shall be for a period of three (3) years commencing as of the Effective Date, unless terminated earlier as provided herein.

4.3 Contractor shall furnish a labor and material bond in the form attached hereto as Exhibit "B," which is attached hereto and incorporated herein by this reference, in an amount equal to one hundred percent (100%) of the total compensation to be paid to Contractor pursuant to this Agreement.

ARTICLE 5 – PAYMENTS TO CONTRACTOR

5.1 Total compensation for Contractor's performance of the Services shall not exceed the amount of Three Hundred Thousand Dollars ($300,000.00). City shall pay Contractor on a time and materials basis up to the not to exceed amount in accordance with Exhibit "C," titled "Price Sheet," which is attached hereto and incorporated herein by reference.

5.2 Contractor shall submit monthly invoices to City describing the Services performed during the preceding month. Contractor's invoices shall include a brief description of the

Services performed, the dates the Services were performed, the number of hours spent and by whom. City shall pay Contractor no later than thirty (30) days after receipt and approval by City of Contractor's invoice.

5.3 Any notice or other communication required, or which may be given, pursuant to this Agreement, shall be in writing. Any such notice shall be deemed delivered (i) on the date of delivery in person; (ii) five (5) days after deposit in first class registered mail, with return receipt requested; (iii) on the actual delivery date if deposited with an overnight courier; or (iv) on the date sent by facsimile or electronic mail transmission (including PDF), if confirmed with a copy sent contemporaneously by first class, certified, registered or express mail; in each case properly posted and fully prepaid to the appropriate address set forth below, or such other address as a Party may provide notice in accordance with this section:

CITY:	CONTRACTOR:
City Clerk City of Redlands 35 Cajon Street P.O. Box 3005 (mailing) Redlands, CA 92373 jdonaldson@cityofredlands.org (909) 798-7531	Erik Simmons, President Three Peaks Corp. P.O. Box 101 Calimesa, CA 92320 Erik@threepeakscorp.com (909) 795-1690

ARTICLE 6 – INSURANCE AND INDEMNIFICATION

6.1 The following insurance coverage required by this Agreement shall be maintained by Contractor for the duration of its performance of the Services. Contractor shall not perform any Services unless and until the required insurance listed below is obtained by Contractor. Contractor shall provide City with certificates of insurance and endorsements evidencing such insurance prior to commencement of the Services. Insurance policies shall include a provision prohibiting cancellation or modification of the policy except upon thirty (30) days prior written notice to City.

A. Workers' Compensation and Employer's Liability insurance in the amount that meets statutory requirements with an insurance carrier acceptable to City, or certification to City that Contractor is self-insured or exempt from the workers' compensation laws of the State of California. Contractor shall execute and provide City with Exhibit "D," titled "Workers' Compensation Insurance Certification," which is attached hereto and incorporated herein by this reference, prior to performance of the Services.

B. Comprehensive General Liability insurance with carriers acceptable to City in the minimum amount of One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) aggregate, for public liability, property damage and personal injury is required. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

C. Business Auto Liability coverage, with minimum limits of One Million Dollars ($1,000,000) per occurrence, combined single limit bodily injury liability and property damage liability. This coverage shall include all Contractor owned vehicles used in connection with Contractor's provision of the Services, hired and non-owned vehicles, and employee non-ownership vehicles. City shall be named as an additional insured and such insurance shall be primary and non-contributing to any insurance or self-insurance maintained by City.

6.2 Contractor shall defend, indemnify, and hold harmless City and its elected and appointed officials, employees and agents from and against any and all claims, losses and liability, including attorneys' fees, arising from injury or death to persons or damage to property occasioned by any negligent act or omission by, or the willful misconduct of, Contractor, or its officers, employees and agents in performing the Services.

ARTICLE 7 – CONFLICTS OF INTEREST

7.1 Contractor covenants and represents that it does not have any investment or interest in any real property that may be the subject of this Agreement or any other source of income, interest in real property or investment that would be affected in any manner or degree by the performance of Contractor's Services. Contractor further covenants and represents that in the performance of its duties hereunder, no person having any such interest shall perform any Services under this Agreement.

7.2 Contractor agrees it is not a designated employee within the meaning of the Political Reform Act because Contractor:

A. Does not make a governmental decision whether to:

(i) approve a rate, rule or regulation, or adopt or enforce a City law;
(ii) issue, deny, suspend or revoke any City permit, license, application, certification, approval, order or similar authorization or entitlement;
(iii) authorize City to enter into, modify or renew a contract;
(iv) grant City approval to a contract that requires City approval and to which City is a party, or to the specifications for such a contract;
(v) grant City approval to a plan, design, report, study or similar item;
(vi) adopt, or grant City approval of, policies, standards or guidelines for City or for any subdivision thereof.

B. Does not serve in a staff capacity with City and in that capacity, participate in making a governmental decision or otherwise perform the same or substantially the same duties for City that would otherwise be performed by an individual holding a position specified in City's Conflict of Interest Code under Government Code section 87302.

7.3 In the event City determines that Contractor must disclose its financial interests, Contractor shall complete and file a Fair Political Practices Commission Form 700, Statement of Economic Interests, with the City Clerk's office pursuant to the written instructions provided by the City Clerk.

ARTICLE 8 – GENERAL CONSIDERATIONS

8.1 In the event any action is commenced to enforce or interpret any of the terms or conditions of this Agreement the prevailing Party shall, in addition to any costs and other relief, be entitled to the recovery of its reasonable attorneys' fees, including fees for the use of in-house counsel by a Party.

8.2 Contractor shall not assign any of the Services, except with the prior written approval of City and in strict compliance with the terms and conditions of this Agreement. Any assignment or attempted assignment without such prior written consent may, in the sole discretion of City, results in City's immediate termination of this Agreement.

8.3 Contractor is for all purposes under this Agreement an independent contractor and shall perform the Services as an independent contractor. Neither City nor any of its agents shall have control over the conduct of Contractor or Contractor's employees, except as herein set forth. Contractor shall supply all necessary tools and instrumentalities required to perform the Services. Assigned personnel employed by Contractor are for its account only, and in no event shall Contractor or personnel retained by it be deemed to have been employed by City or engaged by City for the account of, or on behalf of City. Contractor shall have no authority, express or implied, to act on behalf of City in any capacity whatsoever as an agent, nor shall Contractor have any authority, express or implied, to bind City to any obligation.

8.4 This Agreement may be terminated by City, in its sole discretion, by providing not less than five (5) days prior written notice to Contractor of City's intent to terminate. If this Agreement is terminated by City, an adjustment to Contractor's compensation shall be made, but (i) no amount shall be allowed for anticipated profit or unperformed Services, and (ii) any payment due Contractor at the time of termination may be adjusted to the extent of any additional costs to City occasioned by any default by Contractor. Upon receipt of a termination notice, Contractor shall immediately discontinue its provision of the Services and, within five (5) days of the date of the termination notice, deliver or otherwise make available to City, copies (in both hard copy and electronic form, where applicable) of project related data, design calculations, drawings, specifications, reports, estimates, summaries and such other information and materials as may have been accumulated by Contractor in performing the Services. Contractor shall be compensated on a pro-rata basis for Services completed up to the date of termination.

8.5 Contractor shall maintain books, ledgers, invoices, accounts and other records and documents evidencing costs and expenses related to the Services for a period of three (3) years, or for any longer period required by law, from the date of final payment to Contractor pursuant to this Agreement. Such books shall be available at reasonable times for examination by City at the office of Contractor.

8.6 This Agreement, including the Exhibits incorporated herein by reference, represents the entire agreement and understanding between the Parties as to the matters contained herein, and any prior negotiations, written proposals or verbal agreements relating to such matters are superseded by this Agreement. Except as otherwise provided for herein, any

amendment to this Agreement shall be in writing, approved by City and signed by City and Contractor.

8.7 This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions. The Parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated only in the state courts located in San Bernardino County, California, and the federal courts located in Riverside County, California.

8.8 If one or more of the sentences, clauses, paragraphs or sections contained in this Agreement is declared invalid, void or unenforceable by a court of competent jurisdiction, the same shall be deemed severable from the remainder of this Agreement and shall not affect, impair or invalidate the remaining sentences, clauses, paragraphs or sections contained herein, unless to do so would deprive a Party of a material benefit of its bargain under this Agreement.

IN WITNESS WHEREOF, duly authorized representatives of City and Contractor have signed in confirmation of this Agreement.

CITY OF REDLANDS

By: _____
Mario Saucedo, Mayor

THREE PEAKS CORP.

By: _____
Erik Simmons, President

ATTEST:

_____
Jeanne Donaldson, City Clerk

EXHIBIT "A"

SCOPE OF SERVICES

Screening of Concrete/Dirt Stockpile, Concrete Crushing and Stockpiling

Set up equipment and processing/crushing operation shall be coordinated with the Landfill Manager. The project shall be set up or operated in a location where it shall not interfere with daily operations of the Landfill.

Mobilization of Equipment

Mobilize & demobilize appropriate equipment to screen the existing stockpile of concrete/dirt into various sizes and to crush larger pieces into ¾ inches. The Landfill operating hours for moving equipment in and out are typically 6:00 a.m. to 2:30 p.m. Mobilization/demobilization can take place outside of the normal working hours, including Saturday, provided appropriate arrangements are made in advance with the Landfill Manager.

Concrete Stockpile Screening

Current stockpile is heterogenous and contains estimated 35% to 45% dirt in and a wide variety of concrete chunk sizes with and without reinforcement materials that are recovered shall be managed by the City of Redlands Landfill staff.

Contractor, upon examination of the current stockpile, will be able to identify the most effective means of processing the stockpile. Explosives and blasting are not permitted in the performance of the pre-processing work. Work shall comply with the Landfill's Storm Water Pollution Prevention Plan.

The Contractor shall ensure the work area affected by the stockpile screening will not allow ponding of water.

Concrete Crushing

Concrete pieces regardless of size are to be crushed. Concrete is to be crushed to produce one size of material for use in landfill road building. The Landfill desires material that is the following size:

- ¾ inches

The Landfill will accept crushed, recycled clean hard fill (as defined by OAC 3745-400-05 (A) (NOT INCLUDING ASPHAULT CONCRETE) for use as road building material. The clean, hard fill is to be reasonably free of protruding reinforcing material (i.e. rebar) that if placed in a roadway intended for landfill refuse truck and support vehicle traffic would represent a potential risk for tire puncture, undercarriage or hydraulic line damage, fuel tank compromise, etc. The Landfill reserves the right to reject any material which in its opinion could present such a risk. Removal of any rejected material from the landfill and the appropriate handling/disposition of such materials shall be at the sole expense of the Contractor.

EXHIBIT "B"

LABOR AND MATERIAL BOND

Whereas, the City of Redlands, State of California, and Three Peaks Corp. (hereinafter designated as "Principal") have entered into an agreement (the "Agreement") whereby Principal agrees to set up of equipment and the as-needed processing/crushing operation (the "Work"), which said agreement, dated October 6, 2026, and titled as "Agreement to Perform Non-Professional Services for Improvement to Public Builds and Grounds," is hereby referred to and made a part hereof; and

Whereas, under the terms of the Agreement, Principal is required before commencing the performance of the Work, to file a good and sufficient Labor and Material bond with the City of Redlands to secure the claims to which reference is made in Title 3 (commencing with Section 9550) of Part 6 of Division 4 of the Civil Code of the State of California.

Now, therefore, said Principal and the undersigned as corporate surety, are held firmly bound unto the City and all contractors, subcontractors, laborers, material men and other persons employed in the performance of the Agreement and referred to in the aforesaid Code of Civil Procedure in the sum of Three Hundred Thousand Dollars ($300,000.00) for materials furnished or labor thereon of any kind, or for amounts due under the Unemployment Insurance Act with respect to such work or labor, that said surety will pay the same in an amount not exceeding the amount hereinabove set forth, and also in case suit is brought upon this bond, will pay, in addition to the face amount thereof, costs and reasonable expenses and fees, including reasonable attorneys' fees, incurred by the City in successfully enforcing such obligation, to be awarded and fixed by the court, and to be taxed as costs and to be included in the judgment therein rendered.

It is hereby expressly stipulated and agreed that this bond shall insure to the benefit of any and all persons, companies and corporations entitled to file claims under Title 3 (commencing with Section 9550) of Part 6 of Division 4 of the Civil Code, so as to give a right of action to them or their assigns in any suit brought upon this bond.

Should the condition of this bond be fully performed, then this obligation shall become null and void, otherwise it shall be and remain in full force and effect.

The surety hereby stipulates and agrees that no change, extension of time, alteration or addition to the terms of the Agreement or the specifications accompanying the same shall in any manner affect its obligations on this bond, and it does hereby waive notice of any such change, extension of time, alteration or addition.

[Signatures on next page]

In witness whereof, this instrument has been duly executed by the Principal and surety above named, on _____, 2026.

(SEAL)	(SEAL)
(Contractor)	(Surety) By:
(Signature)	(Signature)
	Address: _____ _____
(Seal and Notarial Acknowledgment of Surety)	Telephone( ) _____

EXHIBIT "C"

Price Sheet

Item No.	Item Description	A Unit	B Estimated Qty.	C Unit Price	D Total Price in Figures (BxC)
1.	Mobilization/Demobilization	Lump Sum	1	$ 7,800 /EA	$ 7,800.00
2.	Concrete Stockpile Screening	Tons	10,000	$ 3.50 /TON	$ 35,000.00
3.	Crushing & Stockpiling	Tons	10,000	$ 5.25 /TON	$ 52,500.00
	Price:			Grand Total:	$ 95,300.00

Total tons produced shall be documented by the contractor. The Landfill reserves the right to verify tonnage and quantities via the on-site landfill scales and/or volumetric survey of the final product piles. Daily belt scale tickets are provided to the Landfill Manager.

These prices shall be inclusive of any and all permit, fees, and/or rentals needed to stage the equipment at the Landfill.

EXHIBIT "D"

WORKERS' COMPENSATION INSURANCE CERTIFICATION

Every employer, except the State, shall secure the payment of compensation in one or more of the following ways:

(a) By being insured against liability to pay compensation by one or more insurers duly authorized to write compensation insurance in this State.

(b) By securing from the Director of Industrial Relations, a certificate of consent to self-insure, either as an individual employer, or as one employer in a group of employers, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his or her employees.

CHECK ONE

_____I am aware of the provisions of Section 3700 of the Labor Code which requires every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code, and I will comply with such provisions before commencing the performance of the work and activities required or permitted under this Agreement. (Labor Code §1861).

_____I affirm that at all times, in performing the work and activities required or permitted under this Agreement, I shall not employ any person in any manner such that I become subject to the workers' compensation laws of California. However, at any time, if I employ any person such that I become subject to the workers' compensation laws of California, immediately I shall provide the City with a certificate of consent to self-insure, or a certification of workers' compensation insurance.

I certify under penalty of perjury under the laws of the State of California that the information and representations made in this certificate are true and correct.

THREE PEAKS CORP.

By:_____ Date: _____

Erik Simmons, President

CITY OF REDLANDS
OFFICE OF THE CITY CLERK
BID OPENING REPORT

The following bid was opened on the **23rd day of June 2026 at 11:00 a.m.** on behalf of the Facilities and Community Services Department for the **As-Needed Crushing of Concrete Stockpile Project. Project No. FCS04162026NA.** The bid amounts have not been checked and are subject to correction after the bids have been completely reviewed.

No.	Plan Holder's Name	Bid Cert Signed	Bid Amount
1	Three Peaks Corp., Calimesa, CA	Yes	$95,300.00
2	American International Environmental Inc., Anaheim, CA	Yes	$98,795.00

Jeanne Donaldson, City Clerk
City of Redlands, California

Emailed: Councilmembers,
City Manager, PIO, Press
Department Head: Tabitha Crocker
Staff: Nathalie Ayala, Louie Miranda

City Council **AGENDA ITEM NO. L3.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Consideration of a Purchase and Sales Agreement with Zachary D. Smith, an individual, for the property located at 21 N. Church Street (Assessor Parcel Number 0171-089-13-0000), and determine that the approval of the Agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's Guidelines implementing the California Environmental Quality Act (Facilities and Community Services Department Director Crocker)

MOTION:

If the City Council determines that staff's recommendation is appropriate, the following motions are provided:

1. I move that the City Council determine that approval of the Agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's guidelines implementing the California Environmental Quality Act; and

2. I move that the City Council approve the Purchase and Sale Agreement with Zachary D. Smith, an individual, for the property located at 21 N. Church Street (Assessor Parcel Number 0171-089-13-0000), for a purchase price in the amount of $50,000.

RECOMMENDATION:

Staff recommends that the City Council determine that approval of the Agreement is exempt from environmental review pursuant to Section 15061(b)(3) of the State's guidelines implementing the California Environmental Quality Act. Staff further recommends that the City Council approve the Purchase and Sale Agreement with Zachary D. Smith, an individual, for which purchase for the property located at 21 N. Church Street (Assessor Parcel Number 0171-089-13-0000) shall be in the amount of $50,000.

DISCUSSION:

On October 21, 2025 the City Council approved Resolution No. 8728 declaring the subject property as surplus land. The Resolution was submitted to the Housing and Community Development Department for review and approval. The City received an unsolicited letter offering to purchase the subject property. The proposed buyer, Zachary D. Smith, stated an intent to relocate a home located at 616 E. State Street (APN 0171-089-02) onto the N. Church Street property. Currently, the property located at 616 E. State Street has several code violations and is slated for demolition.

Determination of General Plan Conformity:

Prior to the acquisition or sale of real property by a local agency, Government Code Section 65402 requires that such acquisition or sale be submitted to the Planning Commission for an evaluation as to its conformity with the General Plan. The proposed sale herein was submitted to the Planning Commission for evaluation on March 10, 2026. The Planning Commission evaluated the proposed sale for General Plan conformity and provided its report through the adoption of Resolution No. 1744. Through the adoption of this resolution, the Commission found that the sale would be in conformance with the General Plan.

The subject property totals 5,355 square feet (or 0.12 acre) and is designated as "Transit Village" on the 2035 General Plan Land Use Map. The Surplus Land Act (Government Code Sections 54220 et seq.) applies to the disposition of land by a local agency. The proposed sale is subject to, and consistent with, the applicable requirements of the Surplus Land Act. The Purchase and Sale Agreement include a purchase price for the property of $50,000, the value is consistent with the appraised value as stated in the attached appraisal report.

Approval of the Purchase and Sale Agreement is exempt from environmental review under the California Environmental Quality Act pursuant to CEQA Guidelines Section 15061(b)(3), the commonsense exemption, because the action involves only a transfer of ownership and will not result in any physical change to the environment. Any future development or change in use would be subject to separate discretionary approvals and environmental review, as required.

ALTERNATIVES:

The City Council may elect not to approve the agreement and direct staff accordingly.

STRATEGIC PLAN:

Not applicable.

SUBMITTED BY:
Tabitha Crocker, Facilities & Community Services Director

RECOMMENDED BY:
Charles M. Duggan Jr., City Manager

REVIEWED BY:
Yvette M. Abich Garcia, City Attorney
Danielle Garcia, Assistant City Manager
Kurt Wilson, Assistant City Manager
James Garland, Finance Director

PREPARED BY:
Marion Cronin, Administrative Analyst

FISCAL IMPACT

Fiscal Year: FY 2025-26

Revenue Generating: Yes

Amount: $50,000

Budgeted Y/N:

Account No.: 101300-4811

Additional Appropriation Required: No

Discussion:

The revenue generated by the sale of this property will be deposited into the City's General Fund.

Attachments

A_Purchase_and_Sale_Agreement-071-089-13_21_N_Church_St_FINAL.pdf
B_Appraisal_21_Church_Street_Redlands_8-23-2026.pdf
C_Map.pdf
D_Offer_Letter-_21_Church_St.pdf
E_Resolution_No1744_APN_0171-089-13-0000.pdf

PURCHASE AND SALE AGREEMENT

AND JOINT ESCROW INSTRUCTIONS

DATED

OCTOBER 6, 2026

BY AND BETWEEN

CITY OF REDLANDS,
a municipal corporation

AS SELLER,

ZACHARY D. SMITH,
An Individual,

AS BUYER

TABLE OF CONTENTS

Page

1. PURCHASE AND SALE; COVENANTS AND USE OBLIGATIONS.....1

1.1 Purchase and Sale 2

1.2 Covenants.....2

1.3 Enforcement/Power of Termination.....2

2. PURCHASE PRICE. 3

2.1 Deposits.....3

2.2 Deposit of Balance.....3

3. ESCROW. 3

3.1 Opening of Escrow 3
3.2 Escrow Instructions.....3
3.3 Termination/Cancellation 4

4. ACTIONS PENDING CLOSING. 4

4.1 Due Diligence. 4
4.2 Title. 5

5. DESCRIPTION OF PROPERTY. 6

5.1 The Real Property 6

6. CONDITIONS TO CLOSING. 7

6.1 Buyer's Closing Conditions.....7
6.2 Seller's Closing Conditions.....8

7. CLOSING. 8

7.1 Closing Date.....8
7.2 Deliveries by Seller.....8
7.3 Deliveries by Buyer 9
7.4 Actions by Escrow Agent 9
7.5 Prorations/Apportionment.....10
7.6 Closing Costs 10
7.7 Closing Statement 11
7.8 Deliveries Outside of Escrow 12

8. SELLER'S REPRESENTATIONS AND WARRANTIES. 12

8.1 Due Organization 12
8.2 Seller's Authority; Validity of Agreements 12
8.3 No Third-Party Rights 12
8.4 Litigation 12
8.5 Zoning and Condemnation 12
8.6 No Violations of Environmental Laws 13
8.7 No Other Commitments 13
8.8 Wells 13

9. BUYER'S REPRESENTATIONS AND WARRANTIES. 13

9.1 Due Organization 13
9.2 Buyer's Authority; Validity of Agreements 13

10. SURVIVAL. 14

11. AS-IS 14

12. RISK OF LOSS 14

12.1 Condemnation 14
12.2 Casualty 15

13. REMEDIES 15

13.1 Default by Seller 15
13.2 Default by Buyer 16

14. BROKERS 17

15. MISCELLANEOUS PROVISIONS 17

15.1 Entire Agreement 17
15.2 Modification; Waiver 17
15.3 Notices 17
15.4 Expenses 18
15.5 Severability 18
15.6 Successors and Assigns 19
15.7 Counterparts 19
15.8 Governing Law; Jurisdiction; 19
15.9 Headings 19
15.10 Time of Essence 19
15.11 Further Assurances 19
15.12 Construction 19
15.13 Attorneys' Fees 20
15.14 Business Days 20

PURCHASE AND SALE AGREEMENT
AND JOINT ESCROW INSTRUCTIONS

THIS PURCHASE AND SALE AGREEMENT AND JOINT ESCROW INSTRUCTIONS (this "Agreement") is made and entered into as of 6th day of October, 2026 (the "Agreement Date"), by and between CITY OF REDLANDS, a municipal corporation ("Seller"), and Zachary D. Smith, an Individual ("Buyer"), for the purpose of setting forth the agreement of the parties and to provide instructions to Escrow Agent with respect to the transaction contemplated by this Agreement. Seller and Buyer are sometimes individually referred to herein as a "Party" and, together, as the "Parties."

RECITALS

A. Seller is the owner of an undivided fee simple interest in certain real property located in the City of Redlands ("City"), San Bernardino County ("County"), State of California, located at 21 N. Church Street, Redlands, California, with Assessor Parcel Number 0171-089-13-0000, and as more particularly described on Attachment "A" attached hereto (the "Land"). The Land, together with any Improvements (as defined in Section 5), are referred to in this Agreement as the "Property."

B. Seller desires to sell, transfer, and convey the Property to Buyer, and Buyer desires to purchase and acquire the Property from Seller, upon and subject to the terms and conditions set forth in this Agreement.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants contained in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Buyer and Seller hereby agree, and instruct Escrow Agent, as follows:

1. PURCHASE AND SALE; COVENANTS AND USE OBLIGATIONS.

1.1 Subject to and upon all of the terms and conditions of this Agreement, Seller agrees to sell, transfer, and convey to Buyer, and Buyer agrees to purchase and acquire from Seller, the Property.

1.2 Covenants. The Buyer covenants and agrees it shall comply with the following (the "Use Obligations"):

(a) Prior to Closing, Buyer shall submit to the City for its review and approval a "Structure Relocation Plan." The Structure Relocation Plan shall include documentation and information that demonstrates, to the Seller's reasonable satisfaction, that the Buyer will relocate the 616 E. State Street Building to the Property in accordance with (a) applicable local, state, and federal laws, (b) reasonable safety precautions, and (c) other terms and conditions required by Seller, in its sole and absolute discretion. If the City, in its sole and absolute discretion, does not provide written approval of the Structure Relocation Plan within ten (10) days of receipt, then it shall be deemed disapproved.

(b) Within three (3) months from the date the grant deed consummating this transaction is recorded in the Official Records of San Bernardino County (the "Official Records"), Buyer shall acquire the structure currently located at and commonly known as 616 E. State Street, Redlands, California (the "616 E. State Street Building").

(c) Within twelve (12) months from the date the grant deed consummating this transaction is recorded in the Official Records, the 616 E. State Street Building shall have been relocated and all rehabilitation shall have been completed in accordance with the Structure Relocation Plan.

(d) Until such time as the obligations of subdivisions (b) and (c) have been completed, the Buyer shall not transfer, lease, assign, or otherwise convey the Property (or portions thereof) to a third party prior to the completion of the proposed Structure Relocation Plan.

(e) Following Close of Escrow, the Property shall be used exclusively for residential purposes allowed by the City of Redlands Municipal Code and any ordinance or regulation affecting the allowable land uses for the Property.

(f) The Use Obligations set forth in this section 1.2 shall survive closing for a period of ten (10) years (the "Restricted Period"), unless earlier terminated in accordance with this Agreement.

1.3 Enforcement of Use Obligations; Power of Termination. In the event the Buyer breaches the Use Obligations during the Restricted Period, Seller shall have the power to terminate the fee interest granted hereunder and to re-enter and take title to the Property, including any improvements thereon, without liability to Buyer for damages or losses of any kind including, but not limited to, any compensation or assistance for relocation other than those damages or losses caused by Seller's gross negligence or intentional misconduct (the "Power of Termination"). The Power of Termination is set forth in the Grant Deed and shall be binding on Buyer and its successors and assigns as covenant running with the land.

(a) If Buyer breaches the Use Obligations, Seller may exercise the Power of Termination by delivering written notice to Buyer. If Buyer does not cure the breach within thirty (30) days after Buyer's receipt of such Seller notice, or if the nature of such violation is such that more than thirty (30) days is reasonably required to complete such cure and Buyer has not commenced a cure within said thirty (30) days and has not diligently completed its cure within ninety (90) days after Buyer's receipt of such Seller notice, Seller may exercise its power of termination as set forth herein. The interest created in Seller by this paragraph shall be a "power of termination" as defined in California Civil Code Section 885.010. Following an uncured breach of any Use Obligation, Seller may exercise this Power of Termination by delivering notice of termination in any manner permitted by law, and tendering payment of the Purchase Price to Buyer. In the event Seller exercises its Power of Termination as set forth herein due to an uncured breach of the Use Obligation by Buyer, and Seller pays to Buyer the Purchase Price, Seller shall take title to the Property free and clear of the use restrictions described herein. The foregoing power of the Seller shall inure to the benefit of the successors and assigns of the Seller for the Restricted Period, and the successors and assigns of the Buyer shall be subject thereto and bound thereby for such period. Unless the Seller has earlier exercised its Power of Termination in

accordance with this Section 1, from and after the expiration date of the Restricted Period, the foregoing use restriction on the Property shall automatically be deemed null and void and without legal effect.

(b) Seller's transfer of the Property to Buyer is subject to the terms, conditions, and covenants set forth in the Grant Deed, including the Use Obligations. For purposes of providing notice hereof, Buyer agrees that the Memorandum of Agreement set forth in Attachment "D" shall be recorded against the Property at Close of Escrow.

(c) Upon completion of the Structure Relocation Plan, and all necessary approvals from the City of Redlands, or any other governmental entity with authority over the work to be completed as part of the Structure Relocation Plan, Buyer may request early termination of the Restricted Period and a release of the Memorandum of Agreement. Seller shall have not less than thirty (30) days to review a proposed release and provide its written consent. If Seller agrees to the release and termination of the Restricted Period, then the Power of Termination shall be deemed null and void and have no further affect, and the release shall be recorded in the Official Records for the County of San Bernardino. The termination of the Restricted Period shall only affect the rights and obligations under this Agreement. Buyer shall be responsible for recording the release and any related recording fees. If Seller does not provide written approval of the proposed release within thirty (30) days as provided for herein, then the release shall be deemed disapproved.

2. PURCHASE PRICE.

The purchase price of the Property (the "Purchase Price") shall be Fifty Thousand Dollars ($50,000.00). The Purchase Price shall be payable as follows:

2.1 Deposits. Within one (1) day following the "Opening of Escrow" (as hereinafter defined), Buyer shall deposit into "Escrow" (as hereinafter defined) the sum of One Thousand Dollars ($1,000.00) (which amount, together with any and all interest earned thereon, shall hereinafter be referred to as the "Deposit"). The Deposit shall be fully refundable through the Due Diligence Termination Date, as defined in Section 4.1.2. From and after the Due Diligence Termination Date, provided Buyer does not elect to terminate this Agreement pursuant to the terms of Section 4.1.2, the Deposit shall become non-refundable, except as specifically provided otherwise herein, and shall be credited against the Purchase Price at Closing.

2.1.1 Refund of Deposit. In the event that Buyer delivers its Feasibility Notice, but subsequently elects to terminate this Agreement due to (a) a Seller Default, as defined in Section 12.1 hereunder, (b) a failure of a Buyer's Condition to Closing, or (c) the occurrence of any other event which by the terms of this Agreement gives rise to Buyer's right to terminate this Agreement and receive a refund of the Deposit, then, subject to the terms of Section 12.1, (i) the Deposit shall be returned by Escrow Agent to Buyer, or to the extent previously released to Seller, and refunded to Buyer by Seller, (ii) this Agreement and the Escrow shall terminate, and (iii) the Parties shall have no further obligation to one another with respect to this Agreement, except with respect to such provisions which by their terms survive the termination of this Agreement.

2.1.2 Interest. The Deposit and any other cash held by Escrow Agent for the benefit of Buyer shall be held in a federally insured interest-bearing account, and the interest shall accrue to Buyer's benefit.

2.2 Deposit of Balance. Buyer shall, at least one (1) business day prior to Closing (as defined in Section 7.1), deposit into Escrow in the form of wire transfer, cash or a certified or bank cashier's check for immediately available funds, the amount of the Purchase Price less the Deposit, plus Buyer's closing costs and Buyer's share of any prorations to be made in accordance with this Agreement.

3. ESCROW.

3.1 Opening of Escrow. Buyer and Seller shall cause an escrow ("Escrow") to be opened with First American Title Company located at 3281 E. Guasti Rd., Suite 400, Ontario, CA 91761, Attention: Kelly Simoneau, Ksimoneau@firstam.com ("Escrow Agent") by delivery to Escrow Agent of a fully executed copy of this Agreement. Escrow Agent shall promptly deliver to Buyer and Seller written notice of the date of the "Opening of Escrow." As used herein, the term "Opening of Escrow" means the day on which Escrow Agent receives a fully executed copy of this Agreement and has notified each Party in writing of such receipt.

3.2 Escrow Instructions. This Agreement shall constitute escrow instructions to Escrow Agent as well as the agreement of the Parties. In the event that any other printed escrow instructions are requested of the Parties and the terms thereof conflict or are inconsistent with any provision of this Agreement or any deed, instrument, or document executed or delivered in connection with the transaction contemplated hereby, the provisions of this Agreement, or such deed, instrument, or document shall control. Escrow Agent is hereby appointed and designated to act as Escrow Agent and instructed to deliver, pursuant to the terms of this Agreement, the documents and funds to be deposited into Escrow as herein provided.

3.3 Termination/Cancellation. Upon any termination or cancellation (the terms being used interchangeably herein) by either of the Parties as expressly allowed under this Agreement (including, without limitation, any deemed termination or cancellation), (a) the Deposit shall be delivered to the Party that this Agreement specifies is entitled thereto; (b) all documents, instruments, and funds delivered into Escrow shall be returned to the Party that delivered the same into Escrow, and (c) the Parties shall thereafter be relieved from further liability hereunder, except with respect to any obligations under this Agreement that are expressly stated to survive any termination of this Agreement. A copy of any notice of termination allowed under this Agreement shall be sent to Escrow Agent by the Party electing to terminate.

4. ACTIONS PENDING CLOSING.

4.1 Due Diligence. Buyer agrees and acknowledges that Seller shall have no obligations under this Agreement to provide Buyer with any documents regarding the Property, and further that Seller has no obligation to provide a Transfer Disclosure Statement under California Civil Code § 1102.2, subdivision (j), or a Natural Hazards Disclosure Report under California Civil Code § 1103.1(a)(9). Notwithstanding the foregoing, Buyer agrees and

acknowledges that, in the event of Closing, Buyer agrees to accept the Property “as is,” “where is,” and with all faults.

4.1.1 Buyer’s Diligence Tests.

4.1.1.1 For thirty (30) days from the date of this Agreement, Buyer and its employees, agents, consultants, and contractors shall be entitled, at Buyer’s sole cost and expense, to: (a) enter onto the Property, at reasonable times during Seller's normal business hours and upon prior written notice to Seller, to perform any inspections, investigations, studies, and tests of the Property (including, without limitation, physical, engineering, soils, geotechnical, and environmental tests) that Buyer deems reasonable; and (b) investigate such other matters pertaining to the Property as Buyer may desire. Notwithstanding the foregoing, Buyer shall not conduct any invasive testing on the Property without the prior written consent of Seller, which consent shall not be unreasonably withheld, delayed or conditioned. Any entry by Buyer onto the Property shall be subject to, and conducted in accordance with, all applicable laws.

4.1.1.2 Buyer shall keep the Property free and clean of any mechanics' liens and indemnify, protect, defend, and hold Seller and Seller’s partners, officers, directors, shareholders, managers, members, agents, employees, and representatives (each an "Indemnified Party" and collectively, the "Indemnified Parties") harmless from and against any and all claims (including, without limitation, claims for mechanic’s liens or materialman’s liens), causes of action, demands, obligations, losses, damages, liabilities, judgments, costs, and expenses (including, without limitation, reasonable attorneys’ fees, charges, and disbursements) (collectively, "Claims") in connection with or arising out of any inspections of the Property carried on by or on behalf of Buyer pursuant to the terms hereof, provided, however, that Buyer shall have no responsibility or liability for (a) the negligence or willful misconduct of any Indemnified Party; (b) any adverse condition or defect on or affecting the Property not caused by Buyer or its employees, agents, consultants, or contractors but discovered or impacted during their inspections including, without limitation, the pre-existing presence or discovery of any matter (such as, but not limited to, any Hazardous Substance (as hereinafter defined)); and/or (c) the results or findings of any inspection.

4.1.1.3 Upon completion of Buyer's inspections, Buyer shall promptly repair any material damage to the Property caused by its entry thereon and restore the Property to substantially the same conditions as it existed prior to Buyer's entry under this Section 4.1.2.

4.1.1.4 The provisions of this Section 4.1.1 shall survive the Closing or the earlier termination of this Agreement.

4.1.2 Buyer’s Termination Right. Buyer shall have the right at any time on or before the date thirty (30) days following the Opening of Escrow (the "Due Diligence Termination Date") to terminate this Agreement by delivering a written notice of such termination to Seller and Escrow Agent if Buyer determines, in its sole and absolute discretion, that the Property is not acceptable to Buyer for any reason. Buyer shall indicate its satisfaction and/or waiver of the Due Diligence condition described in this Section 4.1 by delivering written notice of such satisfaction and/or waiver ("Feasibility Notice") to Seller and Escrow Agent on or prior to the Due Diligence Termination Date. In the event Buyer fails to timely deliver a Feasibility Notice, then this

Agreement and the Escrow shall be automatically deemed terminated. In the event this Agreement is terminated in accordance with this Section, then the Deposit shall be immediately returned to Buyer and the Parties shall thereafter be relieved from further liability hereunder, except with respect to any obligations under this Agreement that are expressly stated to survive any termination of this Agreement.

4.2 Title.

4.2.1 Deliveries by Seller. Within three (3) Business Days after the Opening Escrow, or as soon thereafter as reasonably practical, Seller shall cause First American Title Company ("Title Insurer") to issue and deliver to Buyer (a) a current commitment for an ALTA standard coverage Owner's Policy of Title Insurance for the Property (the "Title Report") and (b) legible copies of all documents referenced therein (collectively with the Title Report, the "Title Documents").

4.2.2 Buyer's Review of Title. Buyer shall have until the date thirty (30) days following the Opening of Escrow ("Title Review Date") to notify Seller in writing of any objection that Buyer may have to any matters reported or shown in any survey or the Title Documents or any amendments or updates thereof (a "Buyer's Objection Letter") (provided, however, that if any such amendments or updates are received by Buyer after or within five (5) Business Days before the Title Review Date, Buyer shall have five (5) Business Days following Buyer's receipt of such amendment or update and copies of all documents referenced therein to notify Seller of objections to matters shown on any such amendment or update that were not disclosed on the previously delivered survey or Title Documents and the Closing Date shall automatically be extended as necessary to facilitate such notice period and any subsequent periods for Seller's response and Buyer's election as provided in subsections (i) and (ii), below). Matters shown as exceptions to coverage in the Title Report (or any amendments or updates thereof) that are not timely objected to by Buyer as provided above shall be deemed to be "Permitted Exceptions." Seller shall cooperate, at no cost to Seller, with Buyer to eliminate matters objected to by Buyer, but, except as set forth in the last sentence of this Section 4.2.2, Seller shall have no obligation to cure or correct any matter objected to by Buyer. On or before the fifth (5th) Business Day following Seller's receipt of Buyer's Objection Letter, Seller may elect, by delivering written notice of such election to Buyer and Escrow Agent ("Seller's Response"), to cause Title Insurer to remove or insure over any matters objected to in Buyer's Objection Letter. If Seller fails to deliver Seller's Response within the period set forth above, it shall be deemed an election by Seller not to cause Title Insurer to so remove or insure over such objections. If Seller elects or is deemed to have elected not to cause Title Insurer to so remove or insure, or if Buyer determines, in its sole discretion, that any proposed endorsement for or insurance over an objected matter is unsatisfactory, then Buyer must elect, by delivering written notice of such election to Seller and Escrow Agent on or before the earlier to occur of (a) the fifth (5th) Business Day following Buyer's receipt of Seller's Response or (b) if no Seller's Response is received by Buyer, the fifth (5th) Business Day following the date on which Seller shall have been deemed to have responded, as provided above, to: (i) terminate this Agreement, in which case the Deposit, to the extent previously deposited in Escrow, shall be immediately returned to Buyer; or (ii) proceed with this transaction, in which event those objected to exceptions or matters that Seller has not elected to cause Title Insurer to so remove or insure shall be deemed to be Permitted Exceptions. In the event

that Buyer fails to make such election on a timely basis, then Buyer shall be deemed to have elected to terminate this Agreement in accordance with the preceding clause (i).

4.2.3 Condition of Title at Closing. Upon the Closing, Seller shall sell, transfer, and convey to Buyer fee simple title to the Property by a duly executed and acknowledged grant deed in the form of Attachment "B" attached hereto (the "Grant Deed"), subject only to the Permitted Exceptions and the reservations and other matters, if any, referenced or described in said Grant Deed.

5. DESCRIPTION OF PROPERTY.

5.1 The Property. As used in this Agreement, the term "Property" shall mean, collectively, all of Seller's right, title, and interest in and to: (a) the Land; (b) all improvements thereon (the "Improvements"); and (c) all of the rights, privileges, appurtenances, hereditaments, easements, reversions, and remainders pertaining to or used in connection with the Land and/or any of the Improvements, including, without limitation, all (i) development rights and credits, air rights, water, water rights, and water stock relating to the Land, (ii) strips and gores, streets, alleys, easements, rights-of-way, public ways, or other rights appurtenant, adjacent, or connected to the Land, and (iii) minerals, oil, gas, and other hydrocarbon substances in, under, or that may be produced from the Land. The conveyance of the Property is subject to conditions and covenants set forth in the Grant Deed.

6. CONDITIONS TO CLOSING.

6.1 Buyer's Closing Conditions. The obligation of Buyer to complete the transaction contemplated by this Agreement is subject to the following conditions precedent (and conditions concurrent, with respect to deliveries to be made by Seller at the Closing) (the "Buyer's Closing Conditions"), which conditions may be waived, or the time for satisfaction thereof extended, by Buyer only in a writing executed by Buyer:

6.1.1 Title. Title Insurer shall be irrevocably and unconditionally prepared and committed to issue to Buyer (with an effective date not earlier than the Closing Date), an ALTA standard coverage owner's policy of title insurance ("ALTA Standard Policy") in favor of Buyer for the Property (a) showing fee title to the Property vested in Buyer, (b) with liability coverage in an amount equal to the Purchase Price, (c) with those endorsements reasonably requested by Buyer including, without limitation, a Mechanic's Lien Endorsement, and (d) containing no exceptions other than the Permitted Exceptions and the reservations and other matters referenced or described in the Grant Deed (the "Owner's Title Policy"). Buyer may, at its expense, obtain from the Title Company an ALTA extended coverage owner's policy provided the issuance of such ALTA form title policy shall not be a condition to Close of Escrow and shall cause no delay to the Close of Escrow. In the event Buyer elects to obtain an ALTA extended coverage policy, Buyer shall obtain an ALTA Survey, at its sole cost and expense, in a timely manner so as to facilitate the issuance of the ALTA extended coverage policy upon the Close of Escrow.

6.1.2 Seller's Due Performance. All of the representations and warranties of Seller set forth in Section 8 shall be true, correct, and complete in all material respects as of the Closing Date, and Seller, on or prior to the Closing Date, shall have complied with and/or

performed all of the obligations, covenants, and agreements required on the part of Seller to be complied with or performed pursuant to the terms of this Agreement on or prior to the Closing.

6.1.3 Physical Condition of Property. The physical condition of the Property shall be substantially the same on the Closing Date as on the Agreement Date, except for reasonable wear and tear and any damages due to any act of Buyer or Buyer's representatives.

6.1.4 Bankruptcy. No action or proceeding shall have been commenced by or against Seller under the federal bankruptcy code or any state law for the relief of debtors or for the enforcement of the rights of creditors, and no attachment, execution, lien, or levy shall have attached to or been issued with respect to Seller's interest in the Property or any portion thereof.

6.1.5 Possession/Removal of Personal Property. Upon the Close of Escrow, Seller shall deliver exclusive possession of the Property to Buyer. Prior to the Close of Escrow Seller shall have the right to remove any or all improvements and Seller's equipment, trade fixtures or other personal property. Any such salvage and removal shall be performed pursuant to all required permits, in accordance with all laws, rules and regulations, and in such manner that the Property is delivered upon the Close of Escrow. Any improvements or personal property of Seller remaining on the Property after the Close of Escrow shall be conclusively deemed abandoned by Seller (the "Abandoned Personal Property"). Seller waives and relinquishes all rights, title, interest and claims in any such Abandoned Personal Property and effective upon abandonment transfers, conveys and assigns all of its right, title and interest in such Abandoned Personal Property to Buyer for disposition as determined by Buyer in Buyer's sole and absolute discretion.

6.2 Seller's Closing Conditions. The obligation of Seller to complete the transaction contemplated by this Agreement is subject to the following conditions precedent (and conditions concurrent, with respect to deliveries to be made by Buyer at the Closing) (the "Seller's Closing Conditions"), which conditions may be waived, or the time for satisfaction thereof extended, by Buyer only in a writing executed by Seller.

6.2.1 All of the representations and warranties of Buyer set forth in Section 9 shall be true, correct, and complete in all material respects as of the Closing Date.

6.2.2 Buyer, on or prior to the Closing Date, shall have complied with and/or performed all of the obligations, covenants, and agreements required on the part of Buyer to be complied with or performed pursuant to the terms of this Agreement on or prior to the Closing.

6.2.3 Seller shall have received written notice from the California Department of Housing and Community Development finding that the disposition of the Property complies with the Surplus Land Act (Gov. Code § 54220 et seq.)

6.2.4 The disposition of the Property is consistent with the General Plan for the City of Redlands and California Government Code § 65402.

6.2.5 This Agreement and the disposition of the Property as provided for herein has complied with any and all applicable requirements under the California

Environmental Quality Act (Cal. Public. Resources Code § 21000 et seq.), and any applicable appeal or challenge period has expired.

6.2.6 Buyer has acquired the 616 E. State Street Building, and Seller has approved the Structure Relocation Plan.

6.2.7 Buyer has obtained all necessary permits and approvals for implementation of the Structure Relocation Plan, including but not limited to: (a) any and all approvals under the California Environmental Quality Act (Cal. Public Resources Code § 21000) and implementing regulations, (b) any review of historical designations or restrictions by a local, state or federal agency or commission. For purposes of this paragraph, there shall be no pending action regarding this Agreement or the Structure Relocation Plan, and the time for any appeal or challenge shall have expired.

7. CLOSING.

7.1 Closing Date. Subject to the provisions of this Agreement, the Closing shall take place no later than thirty (30) days after the Due Diligence Termination Date ("Closing Date")**.** As used herein, the "Closing" shall mean the recordation of the Grant Deed in the Official Records.

7.2 Deliveries by Seller. On or before the Closing Date, Seller, at its sole cost and expense, shall deliver or cause to be delivered into Escrow the following items, documents, and instruments, each dated as of the Closing Date, fully executed and, if appropriate acknowledged, and, if applicable, in proper form for recording:

7.2.1 Grant Deed; Memorandum of Agreement. The Grant Deed conveying the Property to Buyer, and the Memorandum of Agreement;

7.2.2 Non-Foreign Affidavit. A Non-Foreign Affidavit in the form attached hereto as Attachment "C" (the "Non-Foreign Affidavit");

7.2.3 State Affidavit. A California Franchise Tax Board Form 593-C (the "State Affidavit");

7.2.4 Owner's Affidavit. An owner's affidavit or seller's certificate duly executed by Seller in the form customarily required by title insurance companies in the county in which the Property is located, in connection with the issuance of title insurance, to remove standard exceptions for mechanics liens, the gap period from the latest title update of Buyer's title insurance commitment and Parties in possession;

7.2.5 Proof of Authority. Such proof of Seller's authority and authorization to enter into this Agreement and the transaction contemplated hereby, and such proof of the power and authority of the individual(s) executing or delivering any instruments, documents, or certificates on behalf of Seller to act for and bind Seller as may be reasonably required by Title Insurer or Escrow Agent; and

7.2.6 Other. Such other items, documents, and instruments as may be reasonably required by Buyer, Title Insurer, Escrow Agent, or otherwise in order to effectuate the provisions

of this Agreement and the Closing and/or otherwise to fulfill the covenants and obligations to be performed by Seller at the Closing pursuant to this Agreement.

7.3 Deliveries by Buyer. On or before the Closing Date, Buyer, at its sole cost and expense, shall deliver or cause to be delivered into Escrow the following funds and the following items, documents, and instruments, each dated as of the Closing Date, fully executed and, if appropriate acknowledged, and, if applicable, in proper form for recording:

7.3.1 Purchase Price. Cash or other immediately available funds in an amount equal to the unpaid sum of the Purchase Price (less the Deposit) and all of Buyer's share of the Closing Costs (as hereinafter defined) (and otherwise sufficient to close the transaction contemplated herein);

7.3.2 Proof of Compliance with Structure Relocation Plan. Written verification from Buyer to Seller that Buyer has the rights to acquire and relocate the 616 E. State Street Building and will proceed with the Structure Relocation Plan, subject to all conditions imposed therein and by this Agreement; and

7.3.3 Grant Deed; Memorandum of Agreement. The signed, executed Grant Deed and Memorandum of Agreement.

7.3.4 Other. Such other items, documents, and instruments as may be reasonably required by Seller, Title Insurer, Escrow Agent, or otherwise in order to effectuate the provisions of this Agreement and the Closing and/or otherwise to fulfill the covenants and obligations to be performed by Buyer at the Closing pursuant to this Agreement.

7.4 Actions by Escrow Agent. Provided that Escrow Agent shall not have received written notice from Buyer or Seller of the failure of any condition to the Closing or of the termination of the Escrow and this Agreement, when Buyer and Seller have deposited into Escrow the documents and funds required by this Agreement and Title Insurer is irrevocably and unconditionally prepared and committed to issue the Owner's Title Policy in accordance with the terms hereof, Escrow Agent shall, in the order and manner herein below indicated, take the following actions:

7.4.1 Recording. Cause the Grant Deed and any other documents customarily recorded and/or that the Parties hereto may mutually direct to be recorded in the Official Records and obtain conformed copies thereof for distribution to Buyer and Seller.

7.4.2 Funds. Disburse all funds as follows:

7.4.2.1 Pursuant to the Closing Statement (as hereinafter defined), retain for Escrow Agent's own account all escrow fees and costs, disburse to Title Insurer the fees and expenses incurred in connection with the issuance of the Owner's Title Policy, and disburse to any other persons or entities entitled thereto the amount of any other Closing Costs;

7.4.2.2 Disburse to Seller an amount equal to the Purchase Price, less or plus the net debit or credit to Seller by reason of the prorations and allocations of Closing Costs provided for in this Agreement; and

7.4.2.3 Disburse to the Party who deposited the same any remaining funds in the possession of Escrow Agent after the payments pursuant to Sections 7.4.2.1 and 7.4.2.2 above have been completed.

7.4.3 Delivery of Documents. Deliver: (a) to Seller (i) one original of all documents deposited into Escrow (other than the Grant Deed, the other documents recorded pursuant to the terms of this Agreement, the Non-Foreign Affidavit, the State Affidavit and the General Assignment), (ii) one copy of the Non-Foreign Affidavit, the State Affidavit and the General Assignment, and (iii) one conformed copy of each document recorded pursuant to the terms of this Agreement; and (b) to Buyer, (i) one original of all documents deposited into Escrow (other than the Grant Deed and the other documents recorded pursuant to the terms of this Agreement, but including, without limitation, the Non-Foreign Affidavit and the State Affidavit), and (ii) the one conformed copy of each document recorded pursuant to the terms of this Agreement. Originals of any documents recorded at Closing shall be delivered after such recording as indicated thereon.

7.4.4 Owner's Title Policy. Cause Title Insurer to issue or be irrevocably and unconditionally prepared and committed to issue the Owner's Title Policy to Buyer.

7.5 Prorations/Apportionment.

7.5.1 Method of Proration. Taxes and assessments affecting the Property shall be prorated between Buyer and Seller as of the Closing Date based on a 365-day year. All non-delinquent real estate taxes and assessments on the Property, if any, shall be prorated based on the actual current tax bill, but if such tax bill has not yet been received by Seller by the Closing Date or if supplemental taxes are assessed after the Closing for the period prior to the Closing, the Parties shall make any necessary adjustment after the Closing by cash payment to the Party entitled thereto so that Seller shall have borne all real property taxes, including all supplemental taxes, allocable to the period prior to the Closing and Buyer shall bear all real property taxes, including all supplemental taxes, allocable to the period from and after the Closing. If any real property taxes or assessments or any expenses attributable to the Property and allocable to the period prior to the Closing are discovered or billed after the Closing, the Parties shall make any necessary adjustment after the Closing by cash payment to the Party entitled thereto within five (5) Business Days following the discovery thereof or the receipt by any Party of the bill therefor, as the case may be, so that Seller shall have borne all real property taxes, assessments and expenses allocable to the period prior to the Closing and Buyer shall bear all real property taxes, assessments and expenses allocable to the period from and after the Closing.

7.5.2 Survival. The obligations under this Section 7.5 shall survive the Closing and the delivery and recordation of the Grant Deed for the Property.

7.6 Closing Costs. Each Party shall pay its own costs and expenses arising in connection with the Closing (including, without limitation, its own attorneys' and advisors' fees, charges, and disbursements), except the following costs (the "Closing Costs"), which shall be allocated between the Parties as follows:

7.6.1 Escrow Agent's escrow fees and costs shall be paid one-half by Seller and one-half by Buyer;

7.6.2 The cost of the Owner's Title Policy attributable to the standard coverage portion shall be paid by Buyer;

7.6.3 The cost of the Owner's Title Policy attributable to the extended coverage portion shall be paid by Buyer;

7.6.4 The cost of any items required to be provided by Seller, if any, pursuant to Section 4.2.2, shall be paid by Seller, and the costs of any other endorsements to the Owner's Title Policy shall be paid by Buyer;

7.6.5 Seller shall pay the cost of any documentary transfer taxes in connection with the recording of the Grant Deed;

7.6.6 Buyer shall pay all recording costs for recording the Grant Deed; and

7.6.7 All other closing fees and costs shall be charged to and paid by Seller and Buyer in accordance with customary practices in the County.

7.7 Closing Statement. Three (3) Business Days prior to the Closing Date, Escrow Agent shall deliver to each of the Parties for their review and approval a preliminary closing statement (the "Preliminary Closing Statement") setting forth: (a) the proration amounts allocable to each of the Parties pursuant to Section 7.5; and (b) the Closing Costs allocable to each of the Parties pursuant to Section 7.6. Based on each of the Party's comments, if any, regarding the Preliminary Closing Statement, Escrow Agent shall revise the Preliminary Closing Statement and deliver a final, signed version of a closing statement to each of the Parties at the Closing (the "Closing Statement").

7.8 Deliveries Outside of Escrow. Upon the Closing, Seller shall deliver sole and exclusive possession of the Property to Buyer, subject only to the Permitted Exceptions. Effective immediately upon the Closing, any personal property remaining on the Land shall be deemed abandoned and may be removed and disposed of by Buyer at its sole cost and expense. This Section 7.8 shall survive the Closing.

8. SELLER'S COVENANTS, REPRESENTATIONS AND WARRANTIES.

Seller represents, and warrants to and agrees with Buyer, as of the Agreement Date and as of the Closing Date, as follows:

8.1 Due Organization. Seller is a municipal corporation duly formed under the laws of the State of California.

8.2 Seller's Authority; Validity of Agreements. Seller has full right, power, and authority to sell the Property to Buyer as provided in this Agreement and to carry out its obligations hereunder. The individual(s) executing this Agreement and the instruments referenced herein on behalf of Seller has/have the legal power, right, and actual authority to bind Seller to the terms

hereof and thereof. This Agreement is, and all other instruments, documents and agreements to be executed, and delivered by Seller in connection with this Agreement shall be, duly authorized, executed, and delivered by Seller and the valid, binding, and enforceable obligations of Seller (except as enforcement may be limited by bankruptcy, insolvency, or similar laws) and do not, and as of the Closing Date will not result in any violation of, or conflict with, or constitute a default under, any provisions of any agreement of Seller or any mortgage, deed of trust, indenture, lease, security agreement, or other instrument, covenant, obligation, or agreement to which Seller or the Property is subject, or any judgment, law, statute, ordinance, writ, decree, order, injunction, rule, ordinance, or governmental regulation or requirement affecting Seller or the Property.

8.3 No Third-Party Rights. Except as disclosed in the Title Report, Seller is not aware of any leases or occupancy agreements that grant third-Parties any possessory or usage rights to all or any part of the Property.

8.4 Litigation. Seller is not aware of (a) any actions, investigations, suits, or proceedings pending or threatened that affect the Property, the ownership or operation thereof, or the ability of Seller to perform its obligations under this Agreement, and (b) there are no judgments, orders, awards, or decrees currently in effect against Seller with respect to the ownership or operation of the Property that have not been fully discharged prior to the Agreement Date.

8.5 No Violations of Environmental Laws. To Seller's knowledge and except as disclosed in the Property Materials: (a) the Property is not in, nor has it been or is it currently under investigation for violation of any federal, state, or local law, ordinance, or regulation relating to industrial hygiene, worker health and safety, or to the environmental conditions in, at, on, under, or about the Property, including, but not limited to, soil and groundwater conditions ("Environmental Laws"); (b) the Property has not been subject to a deposit of any Hazardous Substance; (c) neither Seller nor any third Party has used, generated, manufactured, stored, or disposed in, at, on, or under the Property any Hazardous Substance; and (d) there is not now in, on, or under the Property any underground or above ground storage tanks or surface impoundments, any asbestos containing materials, or any polychlorinated biphenyls used in hydraulic oils, electrical transformers, or other equipment. Seller hereby assigns to Buyer as of the Closing all claims, counterclaims, defenses, and actions, whether at common law or pursuant to any other applicable federal, state or other laws that Seller may have against any third Party or Parties relating to the existence or presence of any Hazardous Substance in, at, on, under, or about the Property. For purpose of this Agreement, the term "Hazardous Substance" shall be deemed to include any wastes, materials, substances, pollutants, and other matters regulated by Environmental Laws.

8.6 No Other Commitments. Except as may be disclosed in the Title Report, Seller has not made any commitment or representation to any governmental authority, or any adjoining or surrounding property owner, that would in any way be binding on Buyer or would interfere with Buyer's ability to develop and improve the Property, and Seller shall not make any such commitment or representation that would affect the Property or any portion thereof, without Buyer's written consent.

8.7 Actual Knowledge. For purposes hereof, "Seller is not aware" or "to Seller's knowledge," or like terms shall mean the current actual knowledge of Tabatha Crocker, the City's Finance Director, without implying any duty of investigation or inquiry.

8.8 Survival. All of the representations, warranties, and agreements of Seller set forth in this Agreement shall be true upon the Agreement Date, shall be deemed to be repeated at and as of the Closing Date, and shall survive the delivery of the Grant Deed and the Closing for a period of one (1) year. Prior to a termination of this Agreement, Seller shall not take any action, fail to take any required action, or willfully allow or consent to any action that would cause any of Seller's representations or warranties to become untrue. If any representation or warranty of Seller was true as of the date of this Agreement, but is not true as of the Closing Date, then Seller shall disclose this changed fact to Buyer in writing. So long as Seller makes the foregoing disclosure and the change of circumstances regarding the representation or warranty did not arise due to the fault of Seller, then Seller shall not be in breach of this Agreement due to the fact that the representation or warranty has become untrue as of the Closing Date; provided, however, the fact that any representation or warranty under this Section 8 is untrue as of the Closing Date shall still be a failure of a condition pursuant to Section 6.1.2. Notwithstanding the foregoing, if Buyer has actual knowledge of the incorrectness of any representation or warranty set forth in this Section 8 as of the Close of Escrow and Buyer has not elected to terminate this Agreement as provided herein, then Buyer will be deemed to have waived any claim against Seller for the incorrectness of such representation or warranty.

9. BUYER'S REPRESENTATIONS AND WARRANTIES.

Buyer represents and warrants to Seller, as of the Agreement Date and as of the Closing Date, as follows:

9.1 Buyer's Authority; Validity of Agreements. Buyer has full right, power, and authority to purchase and acquire the Property from Seller as provided in this Agreement and to carry out its obligations hereunder. This Agreement is, and all other instruments, documents, and agreements to be executed and delivered by Buyer in connection with this Agreement shall be, duly authorized, executed, and delivered by Buyer and the valid, binding, and enforceable obligations of Buyer (except as enforcement may be limited by bankruptcy, insolvency, or similar laws) and do not, and as of the Closing Date will not, violate any provision of any law, statute, ordinance, rule, regulation, agreement or judicial order to which Buyer is a Party or to which Buyer is subject.

9.2 Indemnification. From and after Closing, Buyer shall defend, indemnify, and hold harmless the Indemnified Parties from any and all claims against any and all Claims in connection with or arising out of Buyer's ownership, use, management, or improvement of the Property, except to the extent required by law for any Claims arising from Seller's gross negligence or willful misconduct.

9.3 Compliance with Structure Relocation Plan. Buyer covenants and warrants that Buyer will comply with the Structure Relocation Plan and complete the relocation of the 616 E. State Street Building to the Property. This covenant shall survive closing and Seller shall have the

right to enforce this covenant through any rights or remedies under this Agreement or otherwise available at law or equity.

10. SURVIVAL. ALL OF THE REPRESENTATIONS, WARRANTIES, AND AGREEMENTS OF BUYER SET FORTH IN THIS AGREEMENT SHALL BE TRUE UPON THE AGREEMENT DATE, SHALL BE DEEMED TO BE REPEATED AT AND AS OF THE CLOSING DATE AND SHALL SURVIVE THE DELIVERY OF THE GRANT DEED AND THE CLOSING FOR A PERIOD OF ONE (1) YEAR; PROVIDED HOWEVER, THAT SELLER'S POWER OF TERMINATION AND THE USE OBLIGATIONS SHALL SURVIVE CLOSING FOR THE RESTRICTED PERIOD AS SET FORTH IN SECTION 1.2. PRIOR TO A TERMINATION OF THIS AGREEMENT, BUYER SHALL NOT TAKE ANY ACTION, FAIL TO TAKE ANY REQUIRED ACTION, OR WILLFULLY ALLOW OR CONSENT TO ANY ACTION THAT WOULD CAUSE ANY OF BUYER'S REPRESENTATIONS OR WARRANTIES TO BECOME UNTRUE. IF ANY REPRESENTATION OR WARRANTY OF BUYER WAS TRUE AS OF THE AGREEMENT DATE, BUT IS NOT TRUE AS OF THE CLOSING DATE, THEN BUYER SHALL DISCLOSE THIS CHANGED FACT TO SELLER IN WRITING. SO LONG AS BUYER MAKES THE FOREGOING DISCLOSURE AND THE CHANGE OF CIRCUMSTANCES REGARDING THE REPRESENTATION OR WARRANTY DID NOT ARISE DUE TO THE FAULT OF BUYER, THEN BUYER SHALL NOT BE IN BREACH OF THIS AGREEMENT DUE TO THE FACT THAT THE REPRESENTATION OR WARRANTY HAS BECOME UNTRUE AS OF THE CLOSING DATE; PROVIDED, HOWEVER, THE FACT THAT ANY REPRESENTATION OR WARRANTY UNDER SECTION 9 IS UNTRUE AS OF THE CLOSING DATE SHALL STILL BE A FAILURE OF A CONDITION PURSUANT TO SECTION 6.2.

11. AS-IS. THE PARTIES HEREBY ACKNOWLEDGE AND AGREE AS FOLLOWS: (A) BUYER IS A SOPHISTICATED BUYER WHO IS FAMILIAR WITH THIS TYPE OF PROPERTY; (B) EXCEPT AS MAY BE SPECIFICALLY SET FORTH IN THIS AGREEMENT, THE DEED, AND/OR ANY OTHER DOCUMENT OR INSTRUMENT DELIVERED BY SELLER AT CLOSING (THE "EXPRESS REPRESENTATIONS"), NEITHER SELLER NOR ANY OF ITS AGENTS, REPRESENTATIVES, BROKERS, OFFICERS, DIRECTORS, SHAREHOLDERS, MEMBERS, OR EMPLOYEES HAS MADE OR WILL MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, WHETHER ORAL OR WRITTEN, EXPRESS OR IMPLIED, WITH RESPECT TO THE PROPERTY; AND (C) THE PROPERTY IS BEING SOLD TO BUYER IN ITS PRESENT "AS IS," "WHEREAS AS," AND "WITH ALL FAULTS" CONDITION. SUBJECT TO THE EXPRESS REPRESENTATIONS AND THE TERMS HEREOF, BUYER WILL BE AFFORDED THE OPPORTUNITY TO MAKE ANY AND ALL INSPECTIONS OF THE PROPERTY AND SUCH RELATED MATTERS AS BUYER MAY REASONABLY DESIRE AND, ACCORDINGLY, SUBJECT TO THE EXPRESS REPRESENTATIONS, BUYER WILL RELY SOLELY ON ITS OWN DUE DILIGENCE AND INVESTIGATIONS IN PURCHASING THE PROPERTY. IN CONNECTION WITH THE FOREGOING, BUYER EXPRESSLY AGREES TO WAIVE ANY AND ALL RIGHTS WHICH BUYER MAY HAVE

UNDER SECTION 1542 OF THE CALIFORNIA CIVIL CODE, WHICH PROVIDES AS FOLLOWS:

> "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR."

12. RISK OF LOSS.

12.1 Condemnation. If, prior to any Closing, all or any portion of the Property is taken by condemnation or eminent domain (or is the subject of pending condemnation or eminent domain action), Seller shall promptly notify Buyer in writing of such fact. In such event, Buyer shall have the option to terminate this Agreement upon written notice to Seller given within ten (10) Business Days after receipt of such notice from Seller, in which event the Deposit shall be returned to Buyer. Notwithstanding the foregoing, Buyer's failure to provide written notice of Buyer's election to terminate within such ten (10) Business Day period shall be deemed Buyer's election to proceed with this Agreement. Prior to any termination or deemed termination of this Agreement, Buyer shall have the right to participate in any proceedings and negotiations with respect to the taking and any transfer in lieu of taking (and Seller shall not consummate any transfer in lieu of taking without Buyer's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed). If Buyer waives the right to terminate this Agreement and elects to proceed with the Closing, then (a) Seller, at, and as a condition precedent to Buyer's obligation to proceed with, the Closing, must: (i) pay to Buyer (or direct Escrow Agent to credit Buyer against the Purchase Price for) the amount of all awards for the taking (and any consideration for any transfer in lieu of taking) actually received by Seller; and (ii) assign to Buyer by written instrument reasonably satisfactory to Buyer all rights or claims to any future awards for the taking (and any consideration for any transfer in lieu of taking); and (b) the Parties shall proceed to the Closing pursuant to the terms hereof without further modification of the terms of this Agreement.

12.2 Casualty. Prior to the Closing and notwithstanding the pendency of this Agreement, the entire risk of loss or damage by earthquake, hurricane, tornado, flood, landslide, fire, sinkhole, contamination by hazardous materials or other casualty shall be borne and assumed by Seller. If, prior to the Closing, any portion of the Property is damaged as a result of any earthquake, hurricane, tornado, flood, sinkhole, landslide, fire, contamination by hazardous materials or other casualty, Seller shall immediately notify Buyer in writing of such fact. In such event, Buyer shall have the option to terminate this Agreement upon written notice to Seller given within ten (10) Business Days after receipt of any such notice from Seller, in which event the Deposit shall be returned to Buyer. Notwithstanding the foregoing, Buyer's failure to provide written notice of Buyer's election to terminate within such ten (10) Business Day period shall be deemed Buyer's election to proceed with this Agreement. Prior to any termination or deemed termination of this Agreement, Buyer shall have the right to participate in any adjustment of the insurance claim. If Buyer waives the right to terminate this Agreement and elects to proceed with the Closing, then (a) Seller, at, and as a condition precedent to Buyer's obligation to proceed with, the Closing, must either: (i) pay to Buyer (or direct Escrow Agent to credit Buyer against the Purchase Price for) the amount of any insurance proceeds actually received by Seller plus the amount of any deductible

under Seller's insurance; or (ii) if no insurance proceeds have been received by Seller, assign to Buyer by written instrument reasonably satisfactory to Buyer all rights or claims to the insurance proceeds and credit Buyer against the Purchase Price for any deductible payable under Seller's insurance policy; and (b) the Parties shall proceed to the Closing pursuant to the terms hereof without further modification of the terms of this Agreement.

13. REMEDIES.

13.1 Default by Seller. If Seller shall breach any material terms or provisions of this Agreement or otherwise fail to perform any of Seller's material obligations under this Agreement at or prior to Closing, and if such failure continues without cure by Seller for five (5) Business Days after Buyer provides Seller and Escrow Agent with written notice thereof (a "Seller Default"), and provided Buyer is not then in default, then Buyer may, as Buyer's sole remedies for such failure, but without limiting Buyer's right to recover attorneys' fees pursuant to Section 14.13 below: (a) waive the effect of such matter and proceed to consummate this transaction; (b) cancel this Agreement and receive a full refund of the Deposit ; or (c) proceed with an action against Seller for specific performance of Seller's obligations under this Agreement.

13.2 Default by Buyer.

(A) PRIOR TO CLOSING. IF, PRIOR TO CLOSING, BUYER SHALL BREACH ANY OF THE TERMS OR PROVISIONS OF THIS AGREEMENT OR OTHERWISE FAIL TO PERFORM ANY OF BUYER'S OBLIGATIONS UNDER THIS AGREEMENT AND IF SUCH FAILURE CONTINUES WITHOUT CURE BY BUYER FOR FIVE (5) BUSINESS DAYS AFTER SELLER PROVIDES BUYER AND ESCROW AGENT WITH WRITTEN NOTICE THEREOF, AND PROVIDED SELLER IS NOT THEN IN DEFAULT, THEN SELLER MAY WAIVE SUCH BREACH AND PROCEED TO CONSUMMATE THIS TRANSACTION IN ACCORDANCE WITH THE TERMS HEREOF, OR SELLER MAY, AS ITS EXCLUSIVE REMEDY, CANCEL THIS AGREEMENT AND RETAIN THE DEPOSIT AS LIQUIDATED DAMAGES. BUYER AND SELLER HAVE DETERMINED AND HEREBY AGREE THAT IT WOULD BE IMPRACTICAL OR EXTREMELY DIFFICULT, IF NOT IMPOSSIBLE, TO ASCERTAIN WITH ANY DEGREE OF CERTAINTY THE AMOUNT OF DAMAGES THAT WOULD BE SUFFERED BY SELLER IF BUYER FAILS TO PERFORM ANY OF ITS OBLIGATIONS IN ACCORDANCE WITH THE PROVISIONS OF THIS AGREEMENT, AND THE PARTIES AGREE THAT A REASONABLE ESTIMATE OF SUCH DAMAGES UNDER THE CIRCUMSTANCES IS AN AMOUNT EQUAL TO THE DEPOSIT. ACCORDINGLY, BUYER AND SELLER AGREE THAT IF BUYER BREACHES ANY OF ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE DEFAULTS HEREUNDER, SELLER MAY RETAIN THE DEPOSIT AS LIQUIDATED DAMAGES. THE PAYMENT AND RETENTION OF THE DEPOSIT AS LIQUIDATED DAMAGES IS NOT INTENDED AS A FORFEITURE OR PENALTY WITHIN THE MEANING OF CALIFORNIA CIVIL CODE SECTIONS 3275 OR 3369, BUT IS INTENDED TO CONSTITUTE LIQUIDATED DAMAGES TO SELLER PURSUANT TO CALIFORNIA CIVIL CODE SECTIONS 1671, 1676 AND 1677.

Seller's Initials _____ Buyer's Initials _____

(B) POST-CLOSING. IF, FOLLOWING CLOSING, BUYER BREACHES ANY OF THE TERMS OR PROVISIONS OF THIS AGREEMENT OR OTHERWISE FAIL TO PERFORM ANY OF BUYER'S OBLIGATIONS UNDER THIS AGREEMENT AND IF SUCH FAILURE CONTINUES WITHOUT CURE, THEN SELLER SHALL HAVE ANY RIGHTS AND REMEDIES ALLOWED UNDER THIS AGREEMENT OR AVAILABLE AT LAW OR EQUITY.

14. BROKERS.

Neither Party has been represented in this transaction by a broker. Each of Buyer and Seller hereby represents and warrants to and agrees with each other that it has not had, and shall not have, any dealings with any third Party to whom the payment of any broker's fee, finder's fee, commission, or other similar compensation ("Commission") shall or may become due or payable in connection with the transaction contemplated hereby. Seller shall indemnify, defend, protect, and hold Buyer harmless for, from, and against any and all Claims incurred by Buyer by reason of any breach or inaccuracy of the representation, warranty, and agreement of Seller contained in this Section. Buyer shall indemnify, defend, protect, and hold Seller harmless from and against any and all Claims incurred by Seller by reason of any breach or inaccuracy of the representation, warranty, and agreement of Buyer contained in this Section. The provisions of this Section shall survive the Closing or earlier termination of this Agreement.

15. MISCELLANEOUS PROVISIONS.

15.1 Entire Agreement. This Agreement, including the attachments hereto, constitutes the entire agreement between Buyer and Seller pertaining to the subject matter hereof and supersedes all prior agreements, understandings, letters of intent, term sheets, negotiations, and discussions, whether oral or written, of the Parties, and there are no warranties, representations, or other agreements, express or implied, made to either Party by the other Party in connection with the subject matter hereof except as specifically set forth herein or in the documents delivered pursuant hereto or in connection herewith.

15.2 Modification; Waiver. No supplement, modification, waiver, or termination of this Agreement shall be binding unless executed in writing by the Party to be bound thereby. No waiver of any provision of this Agreement shall be deemed or shall constitute a waiver of any other provision hereof (whether or not similar), nor shall such waiver constitute a continuing waiver unless otherwise expressly provided.

15.3 Notices. All notices, consents, requests, reports, demands or other communications hereunder (collectively, "Notices") shall be in writing and may be given personally, by registered or certified mail, by electronic mail, by courier, or by Federal Express (or other reputable overnight delivery service) for overnight delivery, as follows:

To Buyer: Zachary D. Smith
1107 Orange Street
Redlands CA 92374
Telephone: (909) 809-2464

Email: zach@ritashaw.net

To Seller: City of Redlands
300 E. State Street, Suite 690
Redlands, California 92373
Attention: City Clerk
Telephone: (909) 798-7531
Email: jdonaldson@cityofredlands.org

To Escrow Agent: First American Title Company
3281 E. Guasti Rd., Suite 400
Ontario, CA 91761
Attention: Kelly Simoneau
Telephone: (909) 510-6206
Email: Ksimoneau@firstam.com

or to such other address or such other person as the addressee Party shall have last designated by Notice to the other Party and Escrow Agent. All Notices shall be deemed to have been given three (3) days following deposit in the United States Postal Service (postage prepaid) or, upon receipt, if sent by overnight delivery service, courier, facsimile transmission (so long as confirmed by the appropriate automatic confirmation page), electronic mail (so long as receipt is acknowledged or otherwise confirmed), or personally delivered. Notice to a Party shall not be effective unless and until each required copy of such Notice is given. The inability to deliver a Notice because of a changed address of which no Notice was given or an inoperative facsimile number for which no Notice was given of a substitute number, or any rejection or other refusal to accept any Notice, shall be deemed to be the receipt of the Notice as of the date of such inability to deliver or rejection or refusal to accept. Any Notice to be given by any Party hereto may be given by legal counsel for such Party. Telephone numbers are provided herein for convenience only and shall not alter the manner of giving Notice set forth in this Section 15.3.

15.4 Expenses. Subject to the provision for payment of the Closing Costs in accordance with the terms of Section 7.6 of this Agreement and of any other provision of this Agreement, whether or not the transaction contemplated by this Agreement shall be consummated, all fees and expenses incurred by any Party hereto in connection with this Agreement shall be borne by such Party.

15.5 Severability. Any provision or part of this Agreement that is invalid or unenforceable in any situation in any jurisdiction shall, as to such situation and such jurisdiction, be ineffective only to the extent of such invalidity and shall not affect the enforceability of the remaining provisions hereof or the validity or enforceability of any such provision in any other situation or in any other jurisdiction.

15.6 Successors and Assigns. Neither Seller nor Buyer shall assign its rights under this Agreement without the consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any such assignment, no assignment shall relieve the

assignor of any obligations or liability under this Agreement. Subject to the foregoing, all of the Parties' rights, duties, benefits, liabilities, and obligations under this Agreement shall inure to the benefit of, and be binding upon, their respective successors and assigns.

15.7 Counterparts. This Agreement may be executed in as many counterparts as may be deemed necessary and convenient, and by the different Parties hereto on separate counterparts, each of which, when so executed, including, without limitation, by .pdf scanned counterparts of any initialed or executed pages delivered via electronic mail, shall be deemed an original, but all such counterparts shall constitute one and the same instrument.

15.8 Governing Law; Jurisdiction. This Agreement shall be governed by and construed under the laws of the State of California without regard to conflicts-of-laws principles that would require the application of any other law. Each Party hereby consents to the exclusive jurisdiction of any court of competent jurisdiction in San Bernardino County in any action related to or arising under this Agreement.

15.9 Headings. The Section headings of this Agreement are for convenience of reference only and shall not be deemed to modify, explain, restrict, alter, or affect the meaning or interpretation of any provision hereof.

15.10 Time of Essence. Time shall be of the essence with respect to all matters contemplated by this Agreement.

15.11 Further Assurances. In addition to the actions recited herein and contemplated to be performed, executed, and/or delivered by Seller and Buyer, during the term of this Agreement and after the Closing, Seller and Buyer agree to perform, execute, and/or deliver or cause to be performed, executed, and/or delivered any and all such further acts, instruments, deeds, and assurances as may be reasonably required to consummate the transaction contemplated hereby. In furtherance of the foregoing, so long as Buyer is not in default under the terms of this Agreement, Seller will cooperate, as reasonably needed, and at no cost to Seller, in Buyer's feasibility review process as reasonably requested by Buyer.

15.12 Construction. As used in this Agreement, the masculine, feminine, and neuter gender and the singular or plural shall each be construed to include the other whenever the context so requires. This Agreement shall be construed as a whole and in accordance with its fair meaning, without regard to any presumption or rule of construction causing this Agreement or any part of it to be construed against the Party causing the Agreement to be written. The Parties acknowledge that each has had a full and fair opportunity to review the Agreement and to have it reviewed by counsel. If any words or phrases in this Agreement have been stricken, whether or not replaced by other words or phrases, this Agreement shall be construed (if otherwise clear and unambiguous) as if the stricken matter never appeared and no inference shall be drawn from the former presence of the stricken matters in this Agreement or from the fact that such matters were stricken.

15.13 Attorneys' Fees. In the event that either Party hereto brings an action or proceeding against the other Party to enforce or interpret any of the covenants, conditions, agreements, or provisions of this Agreement, each party, including the prevailing Party, shall bear its own costs and attorneys' fees. Notwithstanding the foregoing, in any action by Seller to enforce the Use

Obligations or Power of Termination as provided for in Section 1.3, or a default under Section 13.2(B), the prevailing Party shall be entitled to recover reasonable attorneys' fees and costs.

15.14 Business Days. As used herein, the term "Business Day" shall mean a day that is not a Saturday, Sunday, legal holiday, or holiday recognized by Seller. In the event that the date for the performance of any covenant or obligation under this Agreement shall fall on a Saturday, Sunday, or legal holiday, the date for performance thereof shall be extended to the next Business Day. Similarly, in the event that the day for the performance of any covenant or obligation under this Agreement involving Escrow Agent shall fall on a Business Day, the date for performance thereof shall be extended to the next Business Day.

[Signatures on following page]

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year first above written.

SELLER:

CITY OF REDLANDS, a municipal corporation

By:_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

BUYER:

ZACHARY D. SMITH, an Individual

By:_____
Zachary D. Smith

ESCROW AGENT:

The undersigned Escrow Agent hereby accepts the foregoing Purchase and Sale Agreement and Joint Escrow Instructions, agrees to act as Escrow Agent under this Agreement in strict accordance with its terms, agrees to insert as the "Agreement Date" on page 1 hereof, if not otherwise dated, the latest date this Agreement was signed by Seller and Buyer and delivered to Escrow Agent, and agrees to comply with the applicable provisions of the Internal Revenue Code with respect to the transactions contemplated hereby.

First American Title Company

Date:_____

By:_____
Name: Kelly Simoneau
Title: Senior Commercial Escrow Officer

LIST OF ATTACHMENTS

ATTACHMENT "A" DESCRIPTION OF THE PROPERTY

ATTACHMENT "B" GRANT DEED

ATTACHMENT "C" NON-FOREIGN AFFIDAVIT

ATTACHMENT “D” MEMORANDUM OF AGREEMENT

ATTACHMENT "A"

DESCRIPTION OF THE PROPERTY

Real property in the City of Redlands, County of San Bernardino, State of California, described as follows:

Lot 15 TIMMON'S FIRST ADDITION in the City of Redlands, County of San Bernardino, State of California, as per plat recorded in Book 8 of Maps, Page 76, in the Office of the County Recorder of said County.

EXCEPTING THEREFROM the Westerly 10 feet, measured along the North line of said lot, and the Easterly line being parallel to the Westerly line of said lot.

APN: 0171-089-13-0-000

ATTACHMENT "B"

FORM OF GRANT DEED

[SEE FOLLOWING PAGES]

RECORDING REQUESTED BY
AND WHEN RECORDED MAIL TO:

City of Redlands
35 Cajon Street, Suite 4
P.O. Box 3005 mailing
Redlands, California 92373
Attention: Jeanne Donaldson, City Clerk

EXEMPT FROM RECORDING FEES PURSUANT
TO GOVERNMENT CODE SECTION 27383

(Space Above for Recorder's Use)

APN: 0171-089-13 EXEMPT FROM RECORDING FEES PER GOVT. CODE §27383

Documentary Transfer Tax Calculation Appended Hereto

GRANT DEED

PART ONE

FOR GOOD AND VALUABLE CONSIDERATION, the receipt and sufficiency of which is hereby acknowledged, CITY OF REDLANDS, a municipal corporation (the "Grantor"), hereby grants to ZACHARY D. SMITH, an Individual, the real property in the City of Redlands, County of San Bernardino, State of California, described in Exhibit "A" attached hereto and incorporated herein by this reference.

THIS GRANT AND CONVEYANCE IS MADE AND ACCEPTED SUBJECT TO COVENANTS, CONDITIONS, RESTRICTIONS, RESERVATIONS, RIGHTS OF WAY AND EASEMENTS NOW OF RECORD, AND AS FURTHER SET FORTH IN PART TWO OF THIS GRANT DEED

PART TWO

The conveyance of the Property by the Grantor to the Grantee in Part One is subject to the following terms, conditions, covenants and restrictions:

Section 1. Conveyance Subject to Covenants Set forth in Purchase Sale Agreement. The Property is conveyed pursuant to a Purchase Sale Agreement (“Agreement”), pursuant to which Grantee would take title to the Property on the terms and conditions set forth in the Agreement, including but not limited to the “Use Obligations,” as defined therein. The Use Obligations of the Agreement are incorporated into this Grant Deed by this reference and are deemed to be a part of this Grant Deed, as though fully set forth herein, and enforceable through the Power of Termination set forth in Section 6, below.

Section 2. Condition of Property. The Grantee acknowledges and agrees that the Property is conveyed by the Grantor to the Grantee in its "AS IS," "WHERE IS" and "SUBJECT TO ALL FAULTS CONDITION," as of the date of recordation of this Grant Deed, with no warranties, expressed or implied, as to the environmental or other physical condition of the Property, the presence or absence of any patent or latent environmental or other physical condition on or in the Property, or any other matters affecting the Property.

Section 3. Obligation to Refrain from Discrimination**.** The Grantee for itself, its successors and assigns to all or any part or portion of the Property, covenants and agrees that:

3.1 There shall be no discrimination against or segregation of any person, or group of persons, on account of actual or perceived race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, familial status, source of income, disability, veteran or military status, or genetic information, of any person, in the sale, lease, sublease, transfer, use, occupancy, tenure or enjoyment of the Property nor shall the Developer, itself or any person claiming under or through it, establish or permit any such practice or practices of discrimination or segregation with reference to the selection, location, number, use or occupancy of tenants, lessees, sub-tenants, sub-lessees or vendees of the Property. The covenant of this Section 3 shall run with the land of the Property and shall be enforceable against the Grantee and its successors and assigns in perpetuity and be a covenant in the Grant Deed and the Memorandum of Agreement.

3.2 The covenant of this Section 3 shall run with the land of the Property in perpetuity, shall be enforceable against the Grantee and its successors and assigns, and shall be covenants set forth in the Grant Deed.

Section 4. Form of Non-Discrimination and Non-Segregation Clauses. The Grantee for itself, its successors and assigns to all or any part or portion of the Property, covenants and agrees that:

4.1 The Grantee, such successors and such assigns shall refrain from restricting the sale, lease, sublease, rental, transfer, use, occupancy, tenure or enjoyment of the Property (or any portion thereof) on account of actual or perceived race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, familial status, source of income, disability, veteran or military status, or genetic information. All deeds, leases or contracts pertaining to the Property shall contain or be subject to substantially the following non-discrimination or non-segregation covenants:

(a) In deeds: "The grantee herein covenants by and for itself, its successors and assigns, and all persons claiming under or through them, that there shall be no discrimination against or segregation of, any person or group of persons on account of actual or perceived race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, familial status, source of income, disability, veteran or military status, or genetic information, in the sale, lease, sublease, transfer, use, occupancy, tenure, or enjoyment of the premises herein conveyed, nor shall the grantee or any person claiming under or through it, establish or permit any such practice or practices of discrimination or segregation with reference to the selection, location, number, use or occupancy of tenants, lessees, sub-tenants,

sub-lessee, or vendees in the premises herein conveyed. The foregoing covenants shall run with the land."

(b) In leases: "The Lessee herein covenants by and for itself, its successors and assigns, and all persons claiming under or through them, and this lease is made and accepted upon and subject to the following conditions: That there shall be no discrimination against or segregation of any person or group of persons, on account of actual or perceived race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, familial status, source of income, disability, veteran or military status, or genetic information, in the leasing, subleasing, transferring, use, occupancy, tenure, or enjoyment of the premises herein leased, nor shall the lessee itself, or any person claiming under or through it, establish or permit any such practice or practices of discrimination or segregation with reference to the selection, location, number, use, or occupancy, of tenants lessees, sub-lessee, sub-tenants, or vendees in the premises herein leased."

(c) In contracts: "There shall be no discrimination against or segregation of any person or group of persons on account of actual or perceived race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, familial status, source of income, disability, veteran or military status, or genetic information, in the sale, lease, sublease, transfer, use, occupancy, tenure, or enjoyment of the premises herein conveyed or leased, nor shall the transferee or any person claiming under or through it, establish or permit any such practice or practices of discrimination or segregation with reference to the selection, location, number, use, or occupancy, of tenants, lessees, sub-lessees, sub-tenants, or vendees of the premises herein transferred." The foregoing provision shall be binding upon and shall obligate the contracting party or parties and any subcontracting party or parties, or other transferees under the instrument.

4.2 The covenants of this Section 4 shall run with the land of the Property in perpetuity.

Section 5. Maintenance Condition of the Property. The Grantee for itself, its successors and assigns to all or any part or portion of the Property and/or Project, covenants and agrees that:

5.1 The areas of the Property that are subject to public view (including all existing and future improvements, paving, walkways, landscaping, exterior signage and ornamentation) shall be maintained in good repair and a neat, clean and orderly condition, ordinary wear and tear excepted. If there is an occurrence of an adverse condition on any area of the Property that is subject to public view in contravention of the general maintenance standard described above (a "**Maintenance Deficiency**"), then the Grantor shall notify the Grantee in writing of the Maintenance Deficiency. If the Grantee fails to cure or commence and diligently pursue to cure the Maintenance Deficiency within thirty (30) days of its receipt of notice of the Maintenance Deficiency, the Grantor shall have the right to enter the Property and perform all acts necessary to cure the Maintenance Deficiency, or to take any other action at law or in equity that may then be available to the Grantor to accomplish the abatement of the Maintenance Deficiency. Any sum expended by the Grantor for the abatement of a Maintenance Deficiency on the Property pursuant to this Section 5.1 shall become a lien on the Property, as applicable. If the amount of the lien is

not paid within thirty (30) days after written demand for payment from the Grantor to the Grantee, the Grantor shall have the right to enforce the lien in the manner provided in this Section 5.1.

5.2 Graffiti, as this term is defined in Government Code Section 38772, that has been applied to any exterior surface of a structure or improvement on the Property that is visible from any public right-of-way adjacent or contiguous to the Property, shall be removed by the Grantee by either painting over the evidence of such vandalism with a paint that has been color-matched to the surface on which the paint is applied, or graffiti may be removed with solvents, detergents or water, as appropriate. If any such graffiti and is not removed within ninety-six (96) hours following the time of the discovery of the graffiti, the Grantor shall have the right to enter the Property and remove the graffiti, without notice to the Grantee. Any sum expended by the Grantor for the removal of graffiti from the Property pursuant to this Section 5.2, shall be a lien on the Property. If the amount of the lien is not paid within thirty (30) days after written demand to the Grantee from the Grantor, the Grantor shall have the right to enforce its lien in the manner provided in this Section 5.2.

5.3 The Parties further mutually understand and agree that the rights conferred upon the Grantor under this Section 5.3 expressly include a grant by the Grantee of a security interest in the Property with the power to establish and enforce a lien or other encumbrance against the Property or any portion thereof, in the manner provided under Civil Code Sections 2924, 2924b and 2924c, to secure the obligations of the Grantee and it successors under Section 5.1 or Section 5.2, including the reasonable attorneys' fees and costs of the Grantor associated with the abatement of a Maintenance Deficiency or removal of graffiti. For the purposes of the preceding sentence the words "**reasonable attorneys' fees and costs of the Grantor**" mean and include the salaries, benefits and costs of the City Attorney and the lawyers employed in the Office of the City Attorney.

5.4 The provisions of this Section 5.4, shall be a covenant running with the land of the Property, shall be enforceable against the Grantee and its successors and assigns in perpetuity. Nothing in the foregoing provisions of this Section 5 shall be deemed to preclude the Grantee from making any alteration, addition, or other change to any structure or improvement or landscaping on the Property, provided that any such changes comply with applicable zoning and building regulations of the City.

Section 6. Grantor Power of Termination Regarding the Property.

6.1 The Grantor hereby reserves a power of termination (the "Power of Termination") pursuant to Civil Code Sections 885.010, et seq., exercisable by the Grantor, in its sole and absolute discretion, upon thirty (30) calendar days written notice to the Grantee referencing this Section 6.1, to terminate the fee interest of the Grantee in the Property and/or any improvements to the Property and revest such fee title in the Grantor and take possession of all or any portion of such real property and improvements, without compensation to the Grantee, upon the occurrence of an Event of Default by the Grantee following the Close of Escrow for a breach of the Use Obligations set forth in the Agreement. The Power of Termination shall continue for a period expiring on the thirtieth (30th) anniversary of the date of the recording of this Grant Deed.

6.2 The thirty (30) calendar day written notice specified Section 6.1 shall specify the Event of Default by the Grantee triggering the Grantor's exercise of its Power of

Termination. The Grantor shall proceed with its remedy as set forth in Section 6.1 only if the Grantee continues in default for a period of ninety (90) calendar days following such notice or, upon commencing to cure such default, fails to diligently and continuously prosecute said cure to satisfactory conclusion.

6.3 Upon the Grantor's exercise of its Power of Termination pursuant to this Section 6, the Grantee or its successors or assigns shall convey by grant deed to the Grantor title to the Property, as specified in the Grantor's notice pursuant to Section 6.1, and all improvements thereon, in accordance with Civil Code Section 1109, as such code section may hereafter be amended, renumbered, replaced or substituted. Such conveyance shall be duly acknowledged by the Grantee and a notary in a manner suitable for recordation. The Grantor may enforce its rights pursuant to this Section 6.3 by means of an injunctive relief or forfeiture of title action filed in any court of competent jurisdiction.

6.4 IMMEDIATELY FOLLOWING THE THIRTY (30) DAY PERIOD SPECIFIED IN SECTION 6.1, ABOVE, THE GRANTOR, ITS EMPLOYEES AND AGENTS SHALL HAVE THE RIGHT TO REENTER AND TAKE POSSESSION OF THE PROPERTY AND ANY IMPROVEMENTS THEREON, WITHOUT FURTHER NOTICE OR COMPENSATION TO THE GRANTEE. BY INITIALING BELOW, THE GRANTEE HEREBY EXPRESSLY WAIVES, TO THE MAXIMUM EXTENT ALLOWED BY LAW, ANY AND ALL RIGHTS THAT THE GRANTEE MAY HAVE UNDER CALIFORNIA CIVIL CODE SECTION 791 AND CALIFORNIA CODE OF CIVIL PROCEDURE SECTION 1162, AS THOSE STATUTES MAY BE AMENDED, REPLACED, RENUMBERED OR SUBSTITUTED, OR UNDER ANY OTHER STATUTES OR COMMON LAW PRINCIPLES OF SIMILAR EFFECT.

GRANTEE'S INITIALS _____

6.5 THE GRANTEE ACKNOWLEDGES AND AGREES THAT THE GRANTOR'S EXERCISE OF ITS POWER OF TERMINATION AND RIGHT OF REENTRY PURSUANT TO THIS SECTION 6.5 MAY WORK A FORFEITURE OF THE ESTATE IN THE PROPERTY CONVEYED TO THE GRANTEE THROUGH THE GRANT DEED. THE GRANTEE HEREBY EXPRESSLY WAIVES, TO THE MAXIMUM EXTENT ALLOWED BY LAW, ANY AND ALL EQUITABLE AND LEGAL DEFENSES THAT THE GRANTEE MAY HAVE TO SUCH FORFEITURE, INCLUDING, BUT NOT LIMITED TO, THE DEFENSES OF LACHES, WAIVER, ESTOPPEL, SUBSTANTIAL PERFORMANCE OR COMPENSABLE DAMAGES. THE GRANTEE FURTHER EXPRESSLY WAIVES, TO THE MAXIMUM EXTENT ALLOWED BY LAW, ANY AND ALL RIGHTS AND DEFENSES THAT THE GRANTEE MAY HAVE UNDER CALIFORNIA CIVIL CODE SECTION 3275 OR ANY OTHER STATUTE OR COMMON LAW PRINCIPLE OF SIMILAR EFFECT. THE GRANTEE ACKNOWLEDGES THAT THE TERMS AND CONDITIONS OF THE AGREEMENT REFLECT THE POSSIBILITY OF FORFEITURE BY VIRTUE OF THE EXERCISE OF THE GRANTOR'S POWER OF TERMINATION PROVIDED IN THIS SECTION 6.5 AND FURTHER ACKNOWLEDGE THAT IT HAS RECEIVED INDEPENDENT AND ADEQUATE CONSIDERATION FOR ITS WAIVER AND RELINQUISHMENT OF RIGHTS AND REMEDIES PURSUANT TO SECTION 6.4 AND THIS SECTION 6.5.

GRANTEE'S INITIALS _____

Section 7. Covenants Run with the Land of the Property. Each of the covenants and agreements contained in this Grant Deed touch and concern the Property and each of them is expressly declared to be a community development covenant that runs with the land for the benefit of the Grantor or the City of Redlands, and such covenants run with the land in favor of the Grantor for the entire period that such covenants are in full force and effect, regardless of whether the Grantor is or remains an owner of any land or interest in land to which such covenants relate. The Grantor, in the event of any breach of any such covenants, has the right to exercise all of the rights and remedies, and to maintain any actions at law or suits in equity or other proper proceedings, to enforce the curing of such breach, as provided in the Agreement or by law. The covenants contained in this Grant Deed are for the benefit of and are enforceable only by the Grantor, and shall survive the execution and recordation of this Grant Deed, for the time period set forth above for each covenant.

Section 11. Costs and Attorneys' Fees for Enforcement Proceeding. If legal proceedings are initiated to enforce the rights, duties or obligations of any of the covenants set forth in this Grant Deed, then each party shall bear its own attorney fees and costs.

Section 12. Effect of Unlawful Provision; Severability. In the event that any provision of this Grant Deed is held to be invalid or unlawful by a final judgment of a court of competent jurisdiction, such invalidity shall not affect the validity of any other provision of this Grant Deed.

[signature page follows]

IN WITNESS WHEREOF, the Grantor has executed this grant deed as of October 6, 2026.

GRANTOR:

CITY OF REDLANDS, a municipal corporation

By:_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

A notary public or other officer completing this certificate verified only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

On _____, 2026, before me, _____
_____, Notary Public, personally appeared _____
_____, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they/executed the same in his/her/their authorized capacity(ies) and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

_____
Notary Public
In and For Said County and State

CERTIFICATE OF ACCEPTANCE OF
GRANT DEED

The undersigned hereby acknowledges acceptance by _____, an individual, as Grantee under the Grant Deed, of the delivery of the subject Property described in the within Grant Deed from the City of Redlands, subject to the covenants and restrictions set forth herein.

GRANTEE:

ZACHARY D. SMITH

Dated:

_____, 2026

_____
Zachary D. Smith

A notary public or other officer completing this certificate verified only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

On _____, 2026, before me, _____
_____, Notary Public, personally appeared _____
_____, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they/executed the same in his/her/their authorized capacity(ies) and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

_____
Notary Public
In and For Said County and State

Document No. _____

Recorded _____, 2026

STATEMENT OF TAX DUE AND REQUEST THAT TAX DECLARATION NOT BE MADE A PART OF THE PERMANENT RECORD IN THE OFFICE OF THE COUNTY RECORDER (PURSUANT TO SECTION 11932 REVENUE AND TAXATION CODE)

TO: Recorder
County of San Bernardino

Request is hereby made in accordance with the provisions of the Documentary Transfer Tax Act that the amount of the tax due not be shown on the original document which names:

Grantor: CITY OF REDLANDS, a municipal corporation

Grantee: ZACHARY D. SMITH, an Individual

The property described in the accompanying document is located in the City of Redlands, County of San Bernardino.

The amount of tax due on the accompanying document is $_____, computed on the full value of the property conveyed.

(Signature of Grantor or Agent)

CITY OF REDLANDS, a municipal corporation

By:_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

Note: After the permanent record is made, this form will be affixed to the conveying document and returned with it.

EXHIBIT “A” TO GRANT DEED

LEGAL DESCRIPTION OF PROPERTY

Real property in the City of Redlands, County of San Bernardino, State of California, described as follows:

Lot 15 TIMMON'S FIRST ADDITION in the City of Redlands, County of San Bernardino, State of California, as per plat recorded in Book 8 of Maps, Page 76, in the Office of the County Recorder of said County.

EXCEPTING THEREFROM the Westerly 10 feet, measured along the North line of said lot, and the Easterly line being parallel to the Westerly line of said lot.

APN: 0171-089-13-0-000

ATTACHMENT "C" TO PURCHASE AND SALE AGREEMENT

NON-FOREIGN AFFIDAVIT

STATE OF _____)
) ss.
County of _____)

The undersigned, as authorized agent of CITY OF REDLANDS, a municipal corporation ("Transferor"), after being duly sworn upon his oath deposes and says that:

Section 1445 of the Internal Revenue Code provides that a transferee of a U.S. real property interest must withhold tax if the transferor is a foreign person. To inform ZACHARY D. SMITH, an Individual ("Transferee"), that withholding of tax is not required upon the disposition of Transferor's interest in a U.S. real property interest, the undersigned hereby certifies the following:

1. Transferor is not a non-resident alien, foreign corporation, foreign partnership, foreign trust, foreign estate, or other foreign person within the meaning of §1445 and §7701 of the Internal Revenue Code and the treasury regulations promulgated thereunder;

2. Transferor is not a disregarded entity as defined in Treas. Reg. § 1.1445-2(b)(2)(iii);

3. Transferor's U.S. taxpayer identification number is: _____;

4. Transferor's business address is: _____
_____.

Transferor understands that this certification may be disclosed to the Internal Revenue Service by Transferee and that any false statement contained herein could be punished by fine, imprisonment, or both.

Under penalties of perjury Transferor declares that it has examined this certification and to the best of its knowledge and belief this certification is true, correct, and complete. The undersigned agent declares that he has the authority to sign this document on behalf of Transferor.

TRANSFEROR:

CITY OF REDLANDS, a municipal corporation

By:_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

A notary public or other officer completing this certificate verified only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

On _____, 2026, before me, _____
_____, Notary Public, personally appeared _____
_____, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they/executed the same in his/her/their authorized capacity(ies) and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

_____
Notary Public
In and For Said County and State

ATTACHMENT "D" TO PURCHASE AND SALE AGREEMENT

MEMORANDUM OF AGREEMENT

[SEE FOLLOWING PAGES]

RECORDING REQUESTED BY
AND WHEN RECORDED MAIL TO:

City of Redlands
35 Cajon Street, Suite 4
P.O. Box 3005 mailing
Redlands, California 92373
Attention: Jeanne Donaldson, City Clerk

EXEMPT FROM RECORDING FEES PER GOVT. CODE §27383 (Space Above for Recorder's Use)

APN: 0171-089-13

MEMORANDUM OF AGREEMENT

1. This Memorandum of Agreement (the "Memorandum") is signed and recorded by the undersigned regarding the real property and improvements located at 21 N. Church Street, Redlands, California (the "Property"), with Assessor Parcel Number 0171-089-13-0000, and as more particularly described as follows:

> Real property in the City of Redlands, County of San Bernardino, State of California, described as follows:
>
> Lot 15 TIMMON'S FIRST ADDITION in the City of Redlands, County of San Bernardino, State of California, as per plat recorded in Book 8 of Maps, Page 76, in the Office of the County Recorder of said County.
>
> EXCEPTING THEREFROM the Westerly 10 feet, measured along the North line of said lot, and the Easterly line being parallel to the Westerly line of said lot.
>
> APN: 0171-089-13-0-000

2. The Memorandum is recorded to provide constructive notice to all third parties that the undersigned parties have entered into a Purchase and Sale Agreement, dated _____, 2026 (the "Agreement"), incorporated fully herein by reference, regarding the agreement by the City of Redlands (the "City") to transfer the Property to Zachary D. Smith, an individual (the "Buyer"). The Agreement sets forth "Use Obligations," defined herein, that impose covenants on Buyer for the use of the Property. In the event Buyer does not comply with the Use Obligations, City has the right to enforce the Use Obligations or exercise a Power of Termination in accordance with California Civil Code Section 885.010 et seq.

3. Buyer's Use Obligations and the Power of Termination are fully set forth in the Purchase and Sale Agreement available with the City, and covenants that run with the land as set forth in the Grant Deed conveying the Property to Buyer and recorded on or about the same date hereof.

4. The Use Obligations continue for a period of ten (10) years from the date this Memorandum is recorded, unless earlier released by City.

5. The Use Obligations set forth in the Agreement and the Grant Deed shall inure to the benefit of, and shall be binding upon the Parties and their respective successors and permitted assigns.

6. This Memorandum is prepared for the purpose of recordation to give notice of the Agreement and Grant Deed. This Memorandum in no way modifies the provisions of the Agreement or the Grant Deed. In the event of any conflict between the terms of this Memorandum and the Agreement or the Grant Deed, the terms of the Agreement or Grant Deed shall govern.

7. This Memorandum shall be recorded in the Official Records of San Bernardino County, California.

SELLER:

CITY OF REDLANDS, a municipal corporation

By:_____
Mario Saucedo, Mayor

ATTEST:

_____
Jeanne Donaldson, City Clerk

BUYER:

ZACHARY D. SMITH, an Individual

By:_____
Zachary D. Smith

[Seller and Buyer signatures to be acknowledged]

A notary public or other officer completing this certificate verified only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

On _____, 2026, before me, _____
_____, Notary Public, personally appeared _____
_____, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they/executed the same in his/her/their authorized capacity(ies) and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

_____
Notary Public
In and For Said County and State

A notary public or other officer completing this certificate verified only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)
) ss.
COUNTY OF _____)

On _____, 2026, before me, _____
_____, Notary Public, personally appeared _____
_____, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they/executed the same in his/her/their authorized capacity(ies) and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

_____
Notary Public
In and For Said County and State

Appraisal of Real Property

Vacant Lot

SW Corner of Church Street and E State Street
21 Church St.
Redlands, CA 92373
As-Is Date of Value: August 13, 2026

Prepared For:
City of Redlands
c/o Ms. Trish Munoz, MBA
Interim FCS Manager
35 Cajon St., Suite 222
Redlands, CA 92373
Phone: (909) 684-9507
Email:tmunoz@cityofredlands.org

Prepared By:
Towers & Associates
James G. Towers, MAI, AI-GRS, CCIM
P.O Box 7783
Redlands, CA 92375
Office: (909) 335-1735
Direct: (909) 223-9328
E-Mail: jtowers@live.com

Towers & Associates
James G. Towers, MAI, AI-GRS, CCIM
P.O Box 7783
Redlands, CA 92375
Office: (909) 335-1735
Direct: (909) 223-9328
E-mail: jtowers@live.com

August 23, 2026

City of Redlands
C/o: Ms. Trish Munoz, MBA
Interim FCS Manager
35 Cajon Street, Suite 222
Redlands, CA 92373
Email: tmunoz@cityofredlands.org

RE: Appraisal of Real Property
Vacant Lot
SW Corner of Church Street and E. State Street
21 Church St.
Redlands, CA 92373
APN: 0171-089-13

Dear Ms. Munoz,

As requested, I have prepared an appraisal of the real property referenced above. The value reported herein is subject to the assumptions and limiting conditions described in the accompanying report. This report has been prepared under the Appraisal Report option in accordance with the reporting requirements set forth under Standards Rule 2-2(a) of the Uniform Standards of Professional Appraisal Practice (USPAP). I have personally performed the inspection and analysis that form the basis of this report.

The subject of this report is a vacant lot located at the SW corner of Church Street and E. State Street, in the city of Redlands, CA. The subject site is ±5,355 square feet (gross) in size. The site has ±45' of frontage along E. State street and 119' of frontage along Church Street, with paved alley to the rear (south). The site was previously developed but is currently clear of any structures. Based on our conversations with the Redlands City Planning officials, any future development would likely require an additional street dedication of ± 4' in width along Church Street, new curb / gutter along Church Street, and the relocation of two above ground power poles along Church Street. The site is suitable for future residential construction or assemblage with the adjacent site(s) to the west.

This appraisal report has been prepared in accordance with the real estate appraisal regulations, as imposed by the Financial Institution Reform, Recovery, and Enforcement Act of 1989 (FIRREA), and the current Uniform Standards of Professional Appraisal

Practice (USPAP), as promulgated by the Appraisal Standards Board of the Appraisal Foundation.

Based on the investigation and analysis described, and subject to the assumptions and limiting conditions set forth in this report, the **As-Is Market Value** of the **Fee Simple** interest in the subject's real property, as of **August 13, 2026, is**:

FIFTY THOUSAND DOLLARS
$50,000

Extraordinary Assumptions and / or Hypothetical Conditions made during the appraisal process are stated below. We advise the client to consider these issues carefully, as their use may have affected the assignment results.

- **Extraordinary Assumptions: Yes; See Page 2.**
- **Hypothetical Conditions: None**

The accompanying report, of which this letter is a part, contains summary discussions of the data, reasoning, and analysis that were used to develop the opinion of value. It also includes summary descriptions of the subject property, the property's locale, the market for the property type, and the appraisers' opinion of highest and best use.

This report has been prepared for the sole use and benefit of the client and intended users that are specifically identified herein. Neither this report, nor any of the information contained herein, shall be used or relied upon by any person or entity other than those authorized by the client and those named as intended users. Towers & Associates is not responsible for any unauthorized use of or reliance upon this report, its contents, and / or its conclusions.

I appreciate the opportunity to be of service to you and look forward to future consultations at your request.

Respectfully Submitted,

James G. Towers, MAI, AI-GRS, CCIM
Principal – Towers & Associates
Certified General Real Estate Appraiser
California BREA Appraiser Identification Number AG003282 (expires 6/7/2026)

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1
EXTRAORDINARY ASSUMPTIONS AND LIMITING CONDITIONS 2
GENERAL ASSUMPTIONS AND LIMITING CONDITIONS 3
INTRODUCTION 5
SCOPE OF THE APPRAISAL 5
PROPERTY RIGHTS APPRAISED 6
IDENTIFICATION OF CLIENT AND INTENDED USERS OF THE REPORT 7
INTENDED USE OF THE REPORT 7
PURPOSE OF THE APPRAISAL 7
FUNCTION OF THE APPRAISAL 7
PRIOR APPRAISALS AND/OR OTHER SERVICES 7
DEFINITION OF MARKET VALUE 7
PROPERTY IDENTIFICATION 9
LEGAL DESCRIPTION 9
OWNER(S) OF RECORD 9
RECENT SALES HISTORY 9
TAX AND ASSESSMENT ANALYSIS 9
REGIONAL DESCRIPTION 10
COMMUNITY / NEIGHBORHOOD DESCRIPTION 17
MARKET OVERVIEW 20
SITE DESCRIPTION AND ANALYSIS 23
HIGHEST AND BEST USE 35
VALUATION 37
DIRECT SALES COMPARISON APPROACH 38
RECONCILIATION AND CONCLUSION OF AS-IS VALUE 51
ESTIMATE OF MARKETING/ EXPOSURE TIME 52
CERTIFICATION OF APPRAISAL 53
QUALIFICATIONS OF APPRAISER – JAMES G. TOWERS, MAI, AI-GRS, CCIM 54
ADDENDUM 56

EXECUTIVE SUMMARY

PROPERTY SUMMARY	
Address	21 Church St.
City, State, Zip	Redlands, CA 92373
County	San Bernardino
APN:	0171-089-13
Census Tract	81.00
Gross Land / Site Area (SF)	5,355 SF 0.12 acres
Zoning	Specific Plan (SP65) NG2 - Neighborhood General 2
Flood Zone Map Panel, Date	Zone AO 06071C8716H Dated 8/28/2008
Highest & Best Use As-If Vacant	Develop with small-lot residential use
Property Type	Vacant Land
No. of Tenants / Occupants	None
Gross / Rentable Building Area (SF)	0
Remaining Economic Life (Years)	N/A
Current Occupancy	0%
VALUATION SUMMARY	
Effective Date of Value (As-IS)	August 13, 2026
Date of Inspection	August 13, 2026
Date of Report	August 23, 2026
Cost Approach	Excluded
Sales Comparison Approach	$50,000
Income Approach	Excluded
As-Is Market Value	**$50,000**
Net Operating Income @ Market	N/A
Personal Property FF&E Included	N/A
Insurable Value/Replacement Cost New	N/A
Exposure Time	6-12 Months
Marketing Time	6-12 Months

EXTRAORDINARY ASSUMPTIONS AND LIMITING CONDITIONS

An extraordinary assumption is defined as:

> *"An assumption, directly related to a specific assignment, which if found to be false, could alter the appraiser's opinions or conclusions."*[1]

Extraordinary assumptions presume as fact otherwise uncertain information about physical, legal, or economic characteristics of the subject property; or about conditions external to the property, such as market conditions or trends; or about the integrity of data used in an analysis.

Extraordinary assumptions utilized in this appraisal include:

1. **Per public records information, the subject's site size is 5,355 square feet, with site dimensions of ± 45' x 119'. According to officials at the city of Redlands Planning Department, any future development would likely require a street dedication of ± 4' in width along Church Street, new curb / gutter along Church Street, and the relocation of two above ground power poles along Church Street. It is an extraordinary assumption of this report, that the subject site could be developed to its highest and best use subject to the described street dedication and offsite improvements.**

The use of extraordinary assumptions may have affected the appraisal assignment results.

HYPOTHETICAL CONDITIONS

A hypothetical condition is defined as:

> *"A condition, directly related to a specific assignment, which is contrary to what is known by the appraiser to exist on the effective date of the assignment results, but is used for the purpose of analysis."*[2]

Hypothetical conditions are contrary to known facts about physical, legal, or economic characteristics of the subject property; or about conditions external to the property, such as market conditions or trends; or about the integrity of data used in an analysis.

Hypothetical conditions utilized in this report include:

1. **None.**

The use of hypothetical conditions may have affected the appraisal assignment results.

[1] USPAP 2014-2015
[2] USPAP 2104-2015

GENERAL ASSUMPTIONS AND LIMITING CONDITIONS

This report has been made with the following assumptions and limiting conditions. They are critical to the analysis and conclusion contained in this report.

1. This ***Appraisal Report*** is intended to comply with the reporting requirements set forth under Standard Rule 2-2(a) of the Uniform Standards of Professional Appraisal Practice (USPSP). As such, it may not include full discussions of the data, reasoning, and analysis that were used in the appraisal process to develop the appraiser's opinion of value. Supporting documentation concerning the data, reasoning, and analysis is retained in the appraiser's file. The information contained in this report is specific to the needs of the client and for the intended use stated in this report. The appraiser is not responsible for unauthorized use of this report.

2. All proposed improvements are assumed to have been fully completed in a workmanlike manner unless otherwise stated. All proposed construction is assumed to conform to the plans and specifications listed in the appraisal report.

3. The property is appraised free and clear of any or all liens or encumbrances unless otherwise stated. Encumbrances always considered and included in the valuation, where they exist, are: real estate taxes, easements, CC&R's, typical financing (comparable to cash in U. S. dollars), purchase options or sale agreements, signed leases, and unpaid bond debt.

4. Unless otherwise stated in this report, the existence of hazardous substances, including (without limitation) asbestos, mold, polychlorinated biphenyls, petroleum leakage, or agricultural chemicals, which may or may not be present on the property, or other environmental conditions, were not called to the attention of, nor did the appraisers become aware of such during the inspection. The appraisers have no knowledge of the existence of such materials on or in the property unless otherwise stated. The appraiser, however, is not qualified to test such substances or conditions. The value estimate is predicated on the assumption that there is no such condition on or in the property or in such proximity thereto that it would cause a loss in value. No responsibility is assumed for any such conditions, or for any expertise or engineering knowledge required to discover them.

5. Responsible ownership and competent property management are assumed.

6. Information furnished by others is believed to be reliable if it cannot be independently verified by the appraisers (e.g., rent rolls, lease abstracts, operating income and expense histories, etc.). However, no warranty is expressed or implied for the accuracy of such.

7. No responsibility is assumed for the legal description or for matters including legal or title considerations. Title to the property is assumed to be good and marketable unless otherwise stated.

8. All engineering is assumed to be correct. The plot plans and other illustrative material in this report are included only to assist the reader in visualizing the property.

9. It is assumed that there are no hidden or unapparent conditions of the property, subsoil, or structures that render it more or less valuable. No responsibility is assumed for such conditions or for arranging for engineering studies that may be required to discover them.

10. It is assumed that all applicable zoning and use regulations and restrictions have been complied with, unless otherwise stated, defined, and considered in the report.

11. It is assumed that all required licenses, certificates of occupancy, consents, or other legislative or administrative authority from any local, state, or national government, or regulatory agency, or private entity or organization have been or can be obtained or renewed for any use on which the value estimate in this report is based.

12. It is assumed that all entitlements required for development of this property, if applicable, have been or can be obtained.

13. Unless otherwise stated, it is assumed that all public utilities, including--but not limited to--electrical service, natural gas, domestic water supplies, waste water disposal, storm drainage facilities, and telephone service, are available.

14. The appraisers assume that the reader(s) or user(s) of this report has been provided with copies of available building plans, and leases and amendments, if any, encumbering the property.

15. The forecasts, projections, or operating estimates contained herein are based upon current market conditions, anticipated short term supply and demand factors and a continued stable economy. These forecasts are, therefore, subject to changes in future conditions.

16. It is assumed that the utilization of the land and improvements is within the boundaries or property lines of the property described and that there is no encroachment or trespass unless noted in the report.

17. The distribution, if any, of the total valuation in this report between land and improvements applies only under the stated program of utilization. The separate allocations for land and improvements must not be used in conjunction with any other appraisal and are invalid if so used.

INTRODUCTION

SCOPE OF THE APPRAISAL

This is an ***Appraisal Report,*** which is prepared under the reporting requirements set forth in Standards Rule 2-2(a) of the Uniform Standards of Professional Appraisal Practice (USPAP). The report includes discussions of the data, reasoning, and analysis that were used to develop the opinion of value. It also includes descriptions of the subject property, the property's locale, the market for the property type, and the appraiser's opinion of highest and best use. Any data and analysis not presented in the summary appraisal report can be obtained from the appraiser's work file(s) upon request.

Prior to accepting this assignment, the appraiser and client have together identified the appraisal problem to be addressed as being the determination of the following value conclusions:

- **As-Is Market Value (Fee Simple)**
- **Insurable Value**

The subject property was visually inspected along with its environs and relevant market data. The appraiser's inspection of the subject property involved the following:

- James Towers, accompanied by Ryan Towers, conducted an onsite inspection of the subject property without the use of specialized equipment.
- The inspection of the comparable data is typically limited to what can be visually observed from the public street.
- The effective date of the As-Is Market Value reflects the last date of physical inspection.
- The subject's site area was determined from public records.
- Public sources and city resources have been utilized to determine the property's existing zoning and/or to confirm the status of any proposed changes to the zoning.

This appraisal includes the following approaches to value:

- Sales Comparison Approach

Approaches to value that have been omitted from the valuation include:

- The income approach has been excluded as vacant industrial land (or land with improvements nearing the end of their economic lives) appeals primarily to developers. This buyer profile typically does not purchase based on the land's ability to produce income.

- The Cost Approach has been excluded as the existing improvements are at or near the end of their economic lives and have only nominal contributory value.

Existing lease contract(s) and any other encumbrances affecting the subject's value and/or marketability were analyzed in arriving at the concluded estimate(s) of the current market value of the identified property rights, as appraised under the stated valuation premise(s).

The market data collected, evaluated, and analyzed in the valuation of the subject property included site sales data, construction cost data, market rental information (rates, terms, etc.), market expense data, and sales of comparable improved properties, as applicable. Market trends, including the supply of, and demand for, competing properties of this type in the subject's market area were also analyzed. All data has been obtained from sources that the appraiser deems reliable. Where possible and practical, the data has been verified with more than one source including the principals and/or agents involved in the transaction. Public records may also have been used as a source of verification.

This appraisal is intended to comply fully with:

- OCC: 12 CFR, Part 34, Real Estate Lending and Appraisals;
- Interagency Appraisal and Evaluation Guidelines, December 10, 2010;
- The current Uniform Standards of Professional Appraisal Practice ("USPAP") promulgated by the Appraisal Standards Board of the Appraisal Foundation;
- Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA);
- Appraisal Institute Standards of Professional Appraisal Practice;
- Client provided appraisal and evaluation guidelines for Fee Panel Members;

PROPERTY RIGHTS APPRAISED

The valuation of the appraised property pertains only to the land and improvements, and does not include any fixtures, equipment, or personal property located on the premises. The analysis reflects that of the **Fee Simple Estate**; defined as:

"..absolute ownership unencumbered by any other interest or estate; subject only to the limitations imposed by the governmental powers of taxation, eminent domain, police power, and escheat."[3]

[3] The Appraisal of Real Estate. 11th Edition; Appraisal Institute, (Appraisal Institute, 1992, Chicago Illinois), Page 137.

IDENTIFICATION OF CLIENT AND INTENDED USERS OF THE REPORT

The Client and intended user of this report is identified as **City of Redlands**. Other potential users of this report include the client's affiliates, departments, or others specifically designated by the **City of Redlands**.

INTENDED USE OF THE REPORT

Exclusive use of the client for potential sale purposes.

PURPOSE OF THE APPRAISAL

To determine Market Value.

FUNCTION OF THE APPRAISAL

This report is to function as an impartial, independent, opinion of market value for the exclusive use of the client.

PRIOR APPRAISALS AND/OR OTHER SERVICES

Prior to completion of this appraisal assignment, this appraiser **has** completed a prior appraisal report that involved the subject property during the three-year period immediately preceding the agreement to perform this assignment. The prior report is summarized as follows:

Client	Date of Report	Date of Value	Appraised Value
City of Redlands	August 11, 2025	July 31, 2025	$50,000

The current value of $50,000 represents a 0% change from the prior report.

DEFINITION OF MARKET VALUE

In this appraisal report, "market value" is hereby defined and qualified as:

Market Value means the most probable price which a property should bring in a competitive and open market under all conditions requisite to a fair sale, the buyer and seller each acting prudently and knowledgeably, and assuming the price is not affected by undue stimulus. Implicit in this definition is the consummation of a sale as of a specified date and the passing of title from seller to buyer under conditions whereby:

a. *Buyer and seller are typically motivated;*

b. *Both parties are well informed or well advised, and acting in what they consider their own best interests;*

c. A reasonable time is allowed for exposure in the open market;

d. Payment is made in terms of cash in U. S. dollars or in terms of financial arrangements comparable thereto; and,

e. The price represents a normal consideration for the property sold unaffected by special or creative financing or sales concessions granted by anyone associated with the sale.

(Source: Office of the Comptroller of the Currency; 12 CFR, part 34, Subpart C - Appraisals, 34.42 Definitions [g].)

PROPERTY IDENTIFICATION

LEGAL DESCRIPTION

Lot 15 Timmon's First Addition, in the City of Redlands, County of San Bernardino, State of California, as per plat recorded in Book 8 of Maps, Page 76, in the Office of the County Recorder of said County.

Except therefrom the westerly 10 feet, measured along the north line of said lot and the easterly line being parallel to the westerly line of said lot.

OWNER(S) OF RECORD

City of Redlands, a municipal corporation

RECENT SALES HISTORY

Per public records, current ownership obtained title on recorded Doc. No. 2001-0362671. Dated 8/9/2001. No sale transactions are known to have occurred over the prior three-year mandatory reporting period. The subject property is not currently known to be listed for sale nor is the property known to be under contract / in escrow.

TAX AND ASSESSMENT ANALYSIS

The subject property is publicly held real estate and is not subject to taxation as determined by the County Assessor's office.

Tax Summary	
APN	**0171-089-13**
Total Taxable Value ($)	n/a
Base Tax Rate	n/a
Base Taxes ($)	n/a
Special Assessments ($)	n/a
Total Taxes ($)	n/a
Overall Tax Rate	n/a

For privately held real estate the county agency collects taxes on behalf of the following entities: the County, most of the county's incorporated cities, school districts, and all other taxing agencies located in the county including special districts (e.g. flood control districts, sanitation districts, etc.). Property taxes are limited by state law to 1% of the assessed value plus voter-approved obligations and special assessments. If no sale or transfer occurs or now new building takes place, assessments may not increase by more than 2% annually.

REGIONAL DESCRIPTION

The subject property is located in Southern California. This region is made up of six counties that include San Bernardino, Riverside, Ventura, Los Angeles, Orange, and San Diego. These six counties have been, and continue to be, interdependent upon one another for a variety of goods and services.

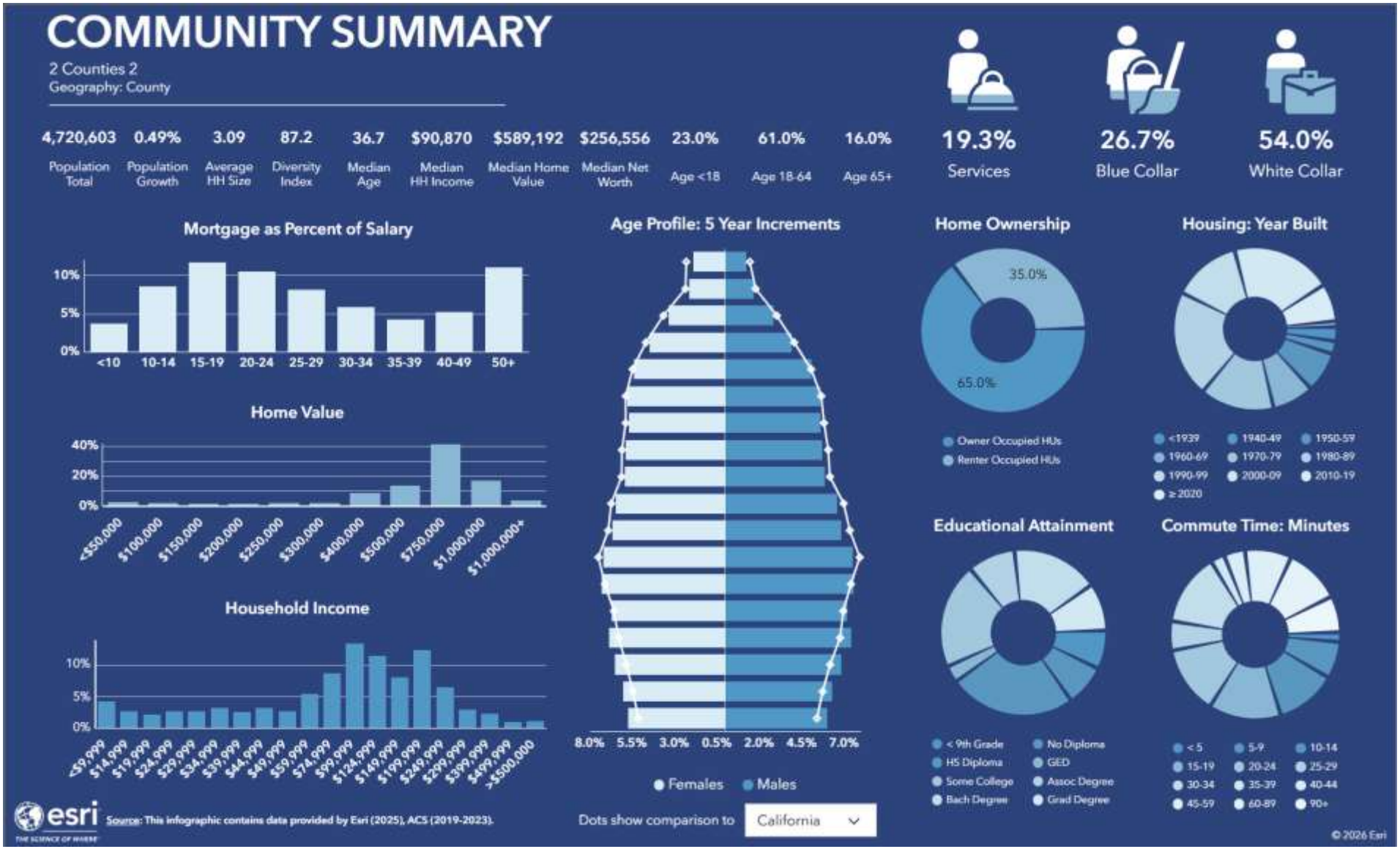
The subject property is located in the Standard Metropolitan Statistical Area (SMSA) commonly referred to as the "Inland Empire" region. The Inland Empire consists primarily of the two counties of San Bernardino and Riverside. Combined, these two counties encompass more than 27,300 square miles, making it the largest SMSA, in terms of land area, in the United States.

The Inland Empire has historically been in the direct path of growth from the greater Los Angeles and Orange County areas. Over the past five decades, the region has experienced a rapid growth rate, ranking as one of the fastest growing regions in the Country. The rapid growth can be attributed in part to affordable real estate in comparison to neighboring Los Angeles and Orange County, an abundance of vacant land available for development, and an extensive network of freeways. The freeway system provides business with the infrastructure necessary for moving goods and services and also allows workers to live in Riverside and San Bernardino counties to commute to the urban employment centers of Los Angeles and Orange County.

Population and Growth

According to U.S. Census statistics, the Inland Empire was officially the fastest-growing region in the State of California between the years 1990 and 2000 and again from 2000 to 2010. Riverside County reportedly grew the fastest of any county in the state (with minimum size threshold of one million populations) while San Bernardino ranked as the third fastest growing county. **According to the January 2026 figures, Riverside County had a population of 2.50 million which reflects a 12.6% increase over the 2010 figures. San Bernardino County's January 2026 population figure was reported at 2.21 million which reflect a 8.1% increase over the 2010 figures**.

On the following page is a Community Profile for the combined Riverside & San Bernardino Counties.


COMMUNITY SUMMARY
2 Counties 2
Geography: County
4,720,603 Population Total
0.49% Population Growth
3.09 Average HH Size
87.2 Diversity Index
36.7 Median Age
$90,870 Median HH Income
$589,192 Median Home Value
$256,556 Median Net Worth
23.0% Age <18
61.0% Age 18-64
16.0% Age 65+
19.3% Services
26.7% Blue Collar
54.0% White Collar
Mortgage as Percent of Salary
10%
5%
0%
<10 10-14 15-19 20-24 25-29 30-34 35-39 40-49 50+
Home Value
40%
20%
0%
<$50,000 $100,000 $150,000 $200,000 $250,000 $300,000 $400,000 $500,000 $750,000 $1,000,000 $1,000,000+
Household Income
10%
5%
0%
<$9,999 $14,999 $19,999 $24,999 $29,999 $34,999 $39,999 $44,999 $49,999 $59,999 $74,999 $99,999 $124,999 $149,999 $199,999 $249,999 $299,999 $399,999 $499,999 >$500,000
Age Profile: 5 Year Increments
8.0% 5.5% 3.0% 0.5% 2.0% 4.5% 7.0%
Females
Males
Dots show comparison to
California
Home Ownership
35.0%
65.0%
Owner Occupied HUs
Renter Occupied HUs
Housing: Year Built
<1939
1940-49
1950-59
1960-69
1970-79
1980-89
1990-99
2000-09
2010-19
≥ 2020
Educational Attainment
< 9th Grade
No Diploma
HS Diploma
GED
Some College
Assoc Degree
Bach Degree
Grad Degree
Commute Time: Minutes
< 5
5-9
10-14
15-19
20-24
25-29
30-34
35-39
40-44
45-59
60-89
90+
esri
Source: This infographic contains data provided by Esri (2025), ACS (2019-2023).
© 2026 Esri

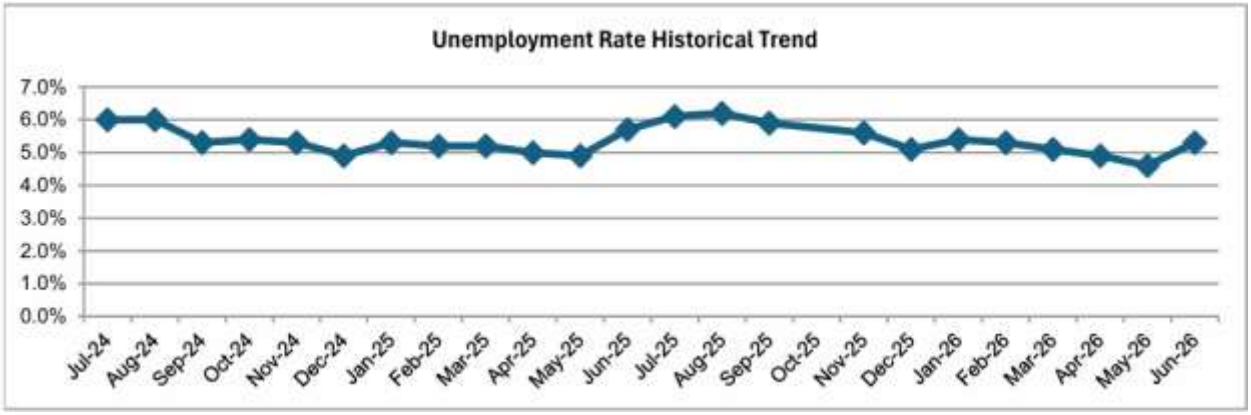
Transportation / Access

The Inland Empire has evolved as a primary transportation and distribution hub for all of Southern California. The area's excellent freeway network, major railroad facilities, and international airport, all provide the ability to process and distribute goods throughout Southern California region and beyond. Interstate 15, 215, and 10 along with State Routes 91, 60, and 210, bisect the region and provide direct access to Los Angeles, Orange, and San Diego Counties, as well as the neighboring states of Nevada and Arizona. Nearly all truck cargo entering or leaving Southern California passes through the Inland Empire. Transportation officials estimate that 35% of all container cargo in the United States passes through the interstate 10 and Interstate 15 corridors. The transcontinental I-10 serves the southern tier of the United States by providing the main east-west link from Santa Monica and Greater Los Angeles in the west to Jacksonville in the east. Major cities served by I-10 include Los Angeles California; Phoenix Arizona; El Paso Texas; San Antonia Texas; Houston Texas; New Orleans Louisiana; and Jacksonville Florida. The Interstate-10 is one of the three coast-to-coast Interstates in the U.S. (the others being Interstates 80 and 90).

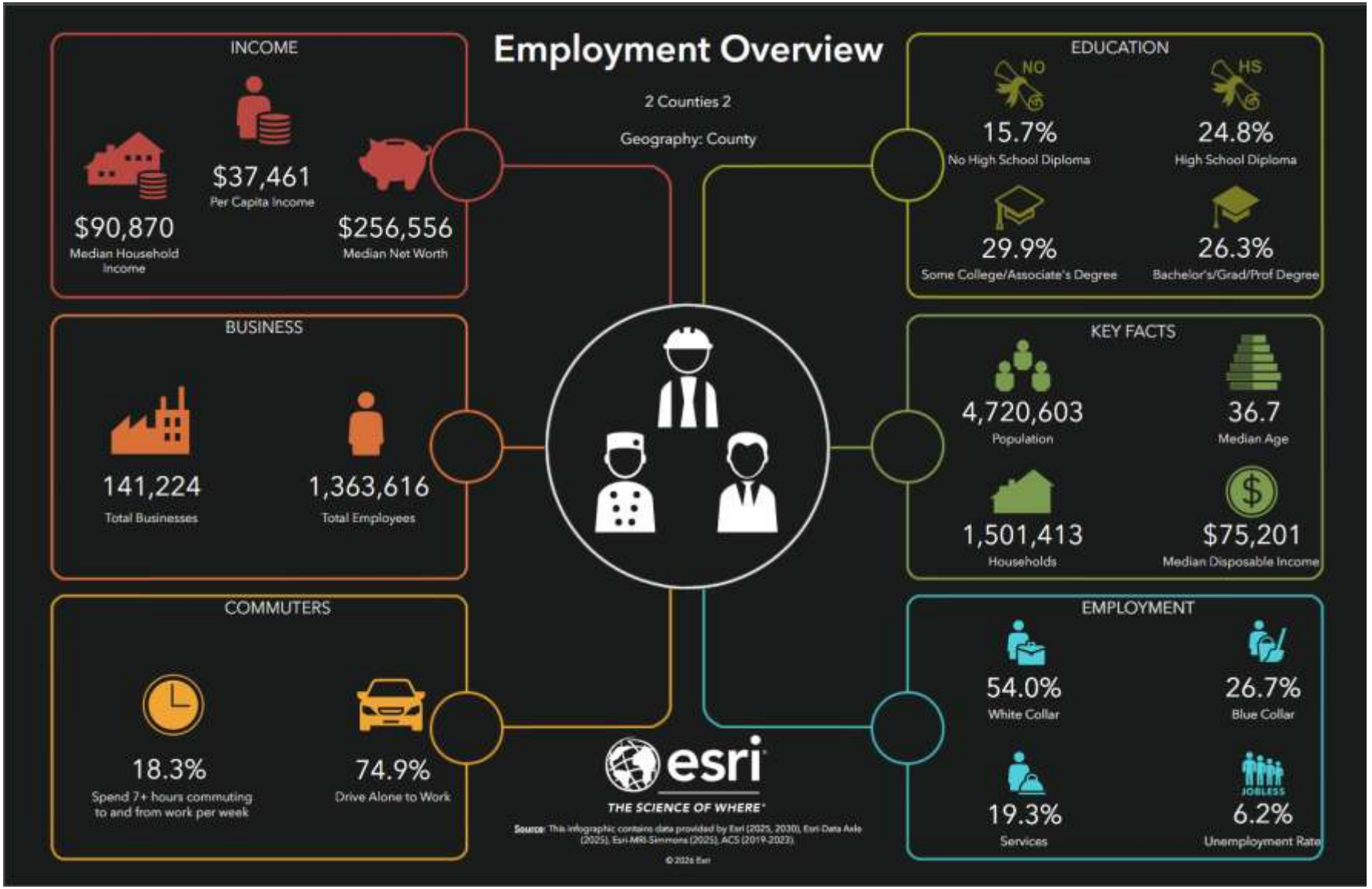
LA / Ontario International Airport (ONT) located in Ontario, is the main airport facility serving the Inland Empire. ONT is a full-service origin and destination airport with commercial jet service to every major city in the United States in addition to serving several foreign countries with direct flights. In terms of cargo, the ONT is second only to LAX in Southern California and has the 15th largest cargo volume in the U.S.

Regional Economic Indicators

The unemployment rate in the Riverside-San Bernardino-Ontario MSA was 5.3 percent in June 2026, up from a revised 4.6 percent in May 2026, and below the year-ago estimate of 5.7 percent. This compares with an unadjusted unemployment rate of 5.2 percent for California and 4.4 percent for the nation during the same period. The unemployment rate was 5.4 percent in Riverside County, and 5.2 percent in San Bernardino County. Between May 2026 and June 2026, total nonfarm employment decreased from 1,722,000 to 1,721,700, a loss of 300 jobs. Agricultural employment increased by 600 jobs. Between June 2025 and June 2026, total nonfarm employment increased by 11,100, a 0.6 percent change. Agricultural employment grew by 800 jobs, or 5.6 percent.



The Inland Empire economy is currently experiencing moderating but continued expansion, reflecting a transition from the rapid growth observed in prior years. The regional Purchasing Managers Index (PMI), published by California State University, San Bernardino Institute of Applied Research, remained firmly in expansionary territory throughout 2025, with recent readings in the mid-60 range, indicating ongoing growth in manufacturing and supply chain-related activity. However, key PMI components such as new orders, production, and employment have shown some deceleration, suggesting that while business conditions remain positive, the pace of growth has slowed. This trend is consistent with broader economic indicators, including modest job growth, softening demand in the logistics and warehousing sector, and rising industrial vacancy rates following a period of significant expansion. At the same time, the region continues to benefit from population growth, relative housing affordability, and ongoing development activity, which support underlying economic stability. Overall, the Inland Empire economy is best characterized as stable with slowing growth, with continued expansion expected at a more measured pace in the near term.


Employment Overview
2 Counties 2
Geography: County
INCOME
$37,461
Per Capita Income
$90,870
Median Household Income
$256,556
Median Net Worth
EDUCATION
NO
15.7%
No High School Diploma
HS
24.8%
High School Diploma
29.9%
Some College/Associate's Degree
26.3%
Bachelor's/Grad/Prof Degree
BUSINESS
141,224
Total Businesses
1,363,616
Total Employees
KEY FACTS
4,720,603
Population
36.7
Median Age
1,501,413
Households
$75,201
Median Disposable Income
COMMUTERS
18.3%
Spend 7+ hours commuting to and from work per week
74.9%
Drive Alone to Work
EMPLOYMENT
54.0%
White Collar
26.7%
Blue Collar
19.3%
Services
JOBLESS
6.2%
Unemployment Rate
esri
THE SCIENCE OF WHERE
Source: This infographic contains data provided by Esri (2025, 2030), Esri-Data Axle (2025), Esri-MRI-Simmons (2025), ACS (2019-2023).
© 2026 Esri

COVID-19 / Post Pandemic Economic Conditions

The long-term economic effects of the COVID-19 pandemic continue to influence the U.S., California, and Inland Empire economies, although the pandemic itself is no longer the primary driver of economic conditions. The most significant legacy has been the inflation and interest-rate cycle that followed the pandemic-era fiscal stimulus, strong consumer demand, labor-market pressures, and global supply-chain disruptions. The resulting increase in inflation prompted the Federal Reserve to undertake one of its most aggressive monetary tightening cycles in decades beginning in 2022. Higher borrowing costs subsequently reduced real estate transaction volume, development activity, and investment demand, particularly during 2023 and 2024.

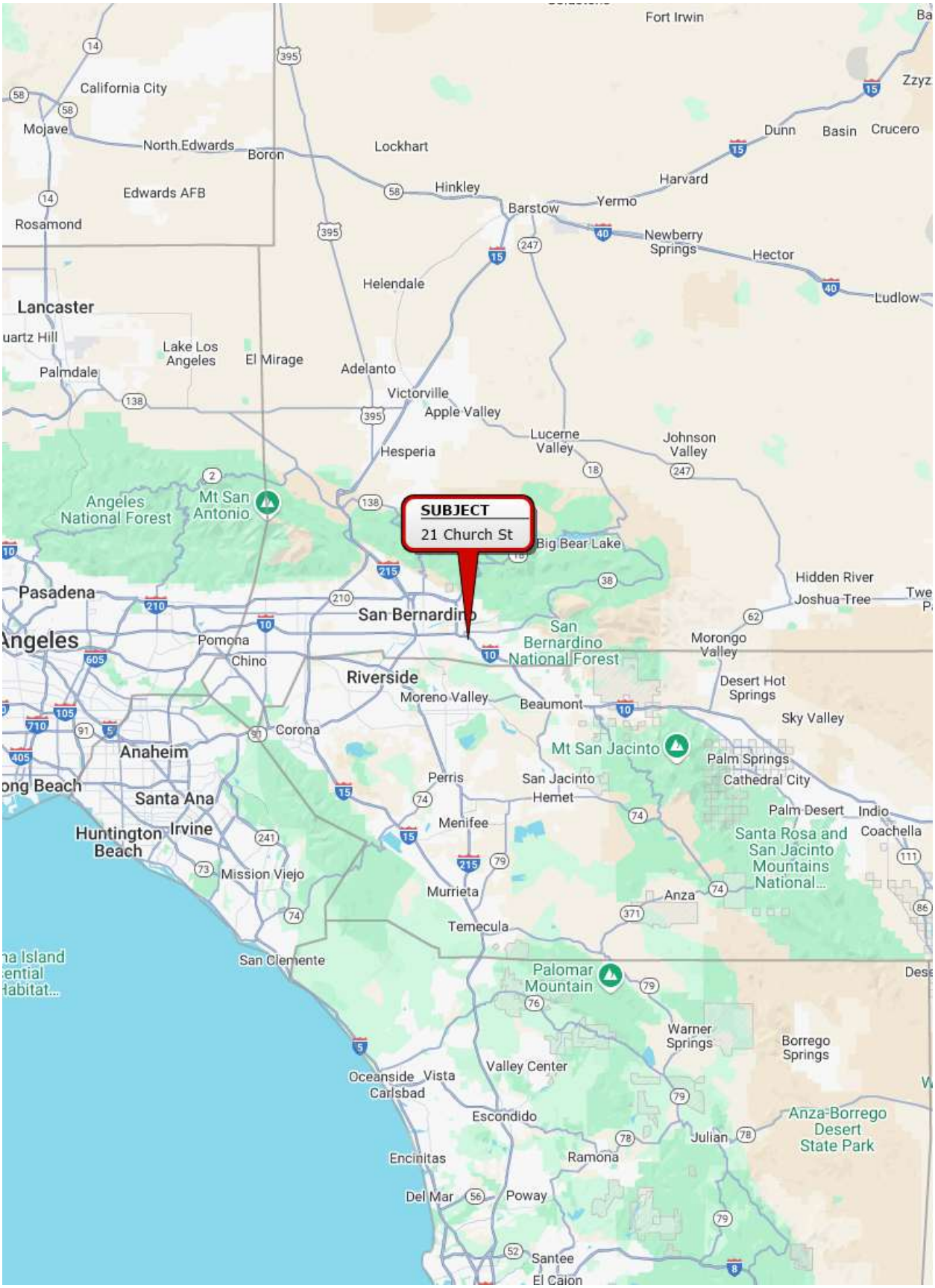
Monetary conditions have since eased materially from their peak, although interest rates remain well above the unusually low levels that prevailed during the pandemic period. As of July 2026, the Federal Reserve's target federal funds rate is 3.50% to 3.75%. The Fed has indicated that inflation remains elevated relative to its 2.0% objective, with the July 2026 Consumer Price Index increasing 3.4% from a year earlier. Consequently, monetary policy remains relatively restrictive and the timing and magnitude of additional rate reductions remain dependent upon inflation, employment, and broader economic conditions.

The Inland Empire economy has generally demonstrated resilience, supported by its large population base, transportation infrastructure, proximity to the ports of Los Angeles and Long Beach, and its established role as a major Southern California logistics and distribution center.

Conclusions

COVID-19 no longer presents a material risk to the region’s economic performance. Instead, macroeconomic factors—most notably inflation, interest rate volatility, and reduced liquidity—are the primary concerns. These conditions have slowed investment activity and heightened investor risk, even as the Inland Empire continues to offer long-term growth prospects due to its strategic location, infrastructure, and demographic trends.

REGIONAL LOCATION MAP



COMMUNITY / NEIGHBORHOOD DESCRIPTION

Community Data

The subject property is located within the city of Redlands. Incorporated in 1888, Redlands is located in the eastern portion of San Bernardino County, approximately 64 miles east of Los Angeles, at the base of the San Bernardino Mountains. Originally settled as an agricultural community, the existing citrus groves, natural areas, and historic architecture lend a small town atmosphere to the city.

Redlands has a wide range of industrial, service, high-tech, and retail businesses. It is no longer reliant upon its historical agriculture industry, although many of the citrus groves still operate in the area. Major employers range from government and high-tech computer services to plastic products manufacturing, to large distribution warehouses. ESRI, a world leader in geographic information system software, is headquartered in Redlands and is one of the largest private employers in the Inland Empire. The health care industry is also a very important segment of the economy, influenced heavily by neighboring Loma Linda University Medical Center, Redlands Community Hospital, Beaver Medical Group (headquartered in Redlands), Kaiser Permanente, and the Veterans Administration Hospital

Excellent educational opportunities have played a large part in the establishment of Redlands as a desirable place to live. The highly regarded University of Redlands has been in existence since 1907. The University is unique in the region in that it houses approximately 80 percent of its students on campus. This large on-campus population along with an on campus faculty of 100 has helped to create what the Redlands Chamber of Commerce refers to as an “Ivy League” quality campus.

According to the California State Department of Finance, the 2010 census figures report the population to be 68,747, which represents an increase of just 8.1% over the 2000 population figures. More recent figures show the January 2025 population at 73,488, which reflects continued population growth of 6.453% since the 2010 census. This relatively slow rate of growth is due in part to a history of slow-growth initiatives passed by the city. While residential growth has, at times, proved somewhat difficult in Redlands, most local area brokers / agents agree there is no market resistance to developing commercial, industrial, or residential property within the city.

	Population			Housing Units							
			Group		Single	Single	Two to		Mobile		Vacancy
City	Total	Household	Qtrs	Total	Detached	Attached	Four	5+ Units	Homes	Occupied	Rate
Redlands	73,488	70,998	2,490	28,318	18,132	1,304	3,122	4,711	1,049	26,863	5.1%

Recent new construction within Redlands includes a wide variety of property types that include retail, multi-family, industrial along with a limited amount of new office space.

Neighborhood Description

Neighborhood Built Up ..... 90% Current Vacancy 5%

Maintenance/Condition..... .....Average
Property Compatibility ....Average
Appeal/Appearance ....Average
Protection/Adverse Influence .....Average
Transportation/Access..... .....Average
Police/Fire Protection ....Average

The subject property is located on the periphery of Downtown Redlands. The subject's immediate neighborhood boundaries are roughly defined as west of University, East of Redlands Boulevard / 9th Street, and south of the I-10 Freeway. This described area is a mix of residential development with commercial / retail uses concentrated along Redlands Blvd. and to a lesser extent along Citrus Avenue. The neighborhood includes the Redlands High School together with its football stadium and baseball fields. The historic Downtown Redlands is directly to the west of the described neighborhood.

The subject property itself is located on the west side of Church Street, ½ block north of Citrus Avenue. Adjacent uses include:

- To the south is Auto Zone, which fronts on Citrus Avenue.
- To the north is a small city-owned lot and older single-family residential homes.
- To the west is an older single-family residential.
- To the east across Church Street, is Redlands High School.

Church Street is a lightly traveled residential street that can become congested when children get dropped off / picked up from Redlands High School. Access to the I-10 Freeway is good with on / off-ramps within one mile of the subject property itself.

Conclusion

Overall, the subject property is well located within a residential neighborhood, which is heavily influenced by the downtown area to the west and Redlands High School to the east. The neighborhood benefits from the good access to the I-10 Freeway and close proximity to the supporting commercial shopping and schools.

NEIGHBORHOOD LOCATION MAP

MARKET OVERVIEW

The California Association of Realtors reports the June 2026 number of sold single family home sales in the Southern California market area (Los Angeles, Riverside, San Diego, Ventura, San Bernardino and Orange counties) were up 20.4% from last month and up 20.6% from a year ago. The average median price paid was $857,279, up slightly 1.79% from $847,680 last month and up 2.6% from June 2025's price of $841,587.

June 2026	Median Sold Price of Existing Single-Family Homes					Sales	
Southern California	26-Jun	26-May	25-Jun	Price MTM% Chg	Price YTY% Chg	Sales MTM% Chg	Sales YTY% Chg
Imperial	$435,000	$417,500	$400,000	4.20%	8.70%	82.50%	69.80%
Los Angeles	$910,370	$838,350	$903,650	8.60%	0.70%	2.60%	6.80%
Orange	$1,490,000	$1,492,500	$1,470,000	-0.20%	1.40%	8.00%	12.20%
Riverside	$635,000	$640,000	$635,000	-0.80%	0.00%	9.50%	7.10%
San Bernardino	$508,080	$486,410	$482,460	4.50%	5.30%	21.10%	13.10%
San Diego	$1,085,000	$1,059,000	$1,025,000	2.50%	5.90%	11.60%	16.10%
Ventura	$937,500	$1,000,000	$975,000	-6.30%	-3.80%	7.50%	19.40%
Average	**$857,279**	**$847,680**	**$841,587**	**1.79%**	**2.60%**	**20.40%**	**20.64%**

The residential housing prices for San Bernardino County have posted modest increases of 4.5% over the past 12 months. Transactions have also increased year of year.

The California Regional Multiple Listing Service was utilized in reviewing the sales activity for the trailing 12 months (8/1/2025-8/1/2026) and includes new homes as well as resales within this immediate market area of the city of Redlands. The data search revealed 643 sales or approximately 54 sales per month. The average home size was 1,958 square feet; the average sale price was $720,493 with an average of 45 days on the market. Statistics are as follows:

Standard Status: Closed (643)

	List Price	DAM	Close Price	SP/LP %	BR	BA	Lot Sqft	SqFt	$/SqFt	Built	Carport Spaces
Min	125,000	0	110,000	75.1 %	1	1	567	567	163.16	1891	
Max	3,395,000	379	3,375,000	125.0 %	10	7	277,913	6,771	673.08	2026	5
Avg	720,493	45	712,947	99.3 %	3	3	12,672	1,958	376.07	1977	1
Median	650,000	26	651,000	100.0 %	3	2	7,800	1,740	370.37	1978	2
Sum	463,277,142		458,425,075						241,812.58		

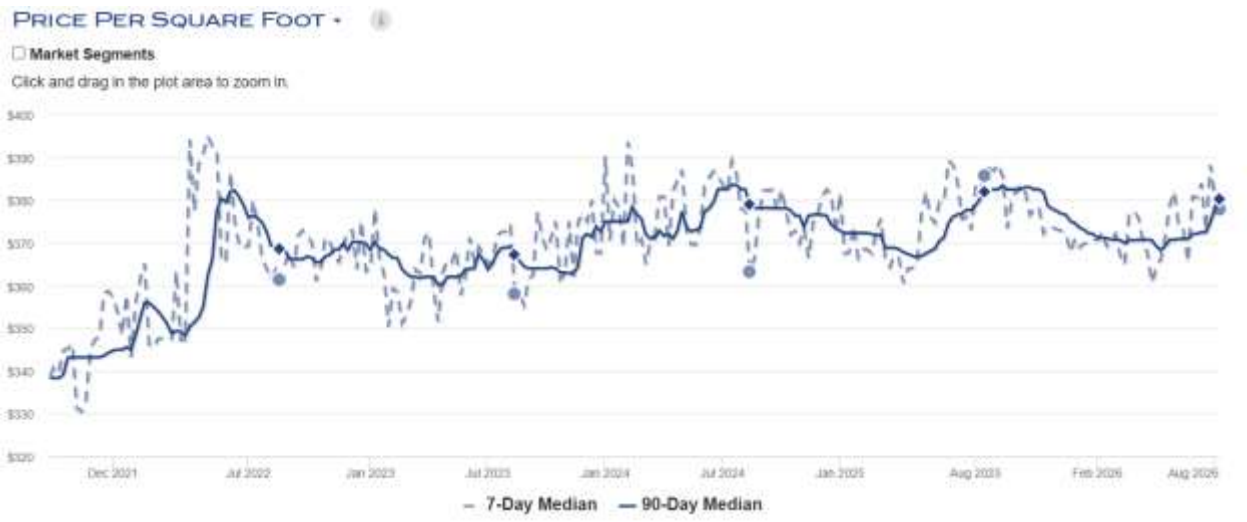
More specifically, a search of all home sales within a ½ mile radius of the subject property was completed. A total of 23 sales were located and indicate a lower average and median price point when compared to all of Redlands. Statistics for are as follows:

Standard Status: Closed (23)

	List Price	DAM	Close Price	SP/LP %	BR	BA	Lot Sqft	SqFt	$/SqFt	Built	Carport Spaces
Min	349,999	0	340,000	90.0 %	1	1	900	888	239.04	1898	2
Max	950,000	188	950,000	107.7 %	5	3	21,344	2,628	575.00	2003	2
Avg	540,986	49	536,247	99.1 %	3	2	6,337	1,511	366.25	1952	2
Median	565,000	26	548,000	100.0 %	3	2	6,359	1,286	340.07	1954	2
Sum	12,442,675		12,333,679						8,423.66		

The statistics suggest that the immediate neighborhood has an older, lower price point than the larger Redlands market.

In general, the market has been cooling over time and prices plateaued in 2022 and have remained relatively stable. The 7-day median list price in Redlands is currently $757,450. The 7-day median price per square foot is currently $378. The market plateau is seen across the price and value. The price per square foot and median listing price have been reasonably stable since mid-2022. The trend line for the price per square foot is as follows:



Individual lot sales are limited in Redlands. During the trailing 12 months, there have been 12 residential lot sales. Statistics for the 12 sales are as follows:

Standard Status: Closed (12)

	List Price	DAM	Close Price	SP/LP %	Lot Sqft	$/SqFt
Min	10,000	2	32,000	80.0 %	6,419	0.07
Max	1,300,000	1343	1,200,000	320.0 %	477,418	21.14
Avg	384,500	249	360,833	111.3 %	133,373	10.67
Median	320,000	66	287,500	94.1 %	34,223	10.53
Sum	4,613,999		4,330,000			128.01

Interviews with Market Participants

We interviewed market participants for this and other recent appraisal assignments to obtain their opinions on the Inland Empire market. Specific responses included the following:

- Inflationary pressure and higher interest rates continue to drag on investors and developers of individual lots as well as bulk lot / subdivisions.

- Construction costs continue to be high and entitlement periods are long, which reduces the number of small investors or contractors looking to purchase individual lots for development,

- Interest rates remain high, which has made qualifying for entry level buyers difficult.

Development Potential

The development potential for the subject property is limited by its small size. As of the date of value, the subject property has no approved entitlements processed through the city of Redlands. The entitlement process is lengthy (12 to 24 months) with developers suggesting a realistic time frame for processing entitlements for a residential lot would be approximately two years.

The subject site is positioned immediately adjacent to older residential housing and across the street from the Redlands High School. Utilities are known to be available to the site. No cost estimates have been made for development of the onsite infrastructure (i.e., streets, utilities, grading, etc.)

Given the subject's location, topography, and lot size, the site would likely support a small single home for an entry-level buyer. To determine exactly what product should be constructed goes beyond the scope of this report.

Market Conclusions

As of mid-2026, the elevated construction costs, persistently high interest rates have created an immediate negative impact on the residential real estate market and by extension the market for residential lots / land. The challenges have resulted in moderately declining land values over the past two to three years.

Most Likely Buyer

Given the subject property's physical characteristics and development potential the most likely buyer would be a developer looking to build an entry-level residential home.

SITE DESCRIPTION AND ANALYSIS

The subject property consists of a single parcel of land at the southwest corner of Church Street and State Street. The site was previously developed with an older tri-plex but is currently a vacant site having been cleared of all structures. The subject site is summarized as follows:

SITE SUMMARY	
Address	21 Church St.
City, State, Zip	Redlands, CA 92373
County	San Bernardino
APN:	0171-089-13
Census Tract	81.00
Gross Land Area	5,355 SF 0.12 acres
Shape	Rectangular
Utility	Average
Dimensions	±45' x 119'
Street Frontage	119' on Church st., 45' on E State st.
Street	Publicly maintained and asphalt paved
Curb/Gutters	Cut stone with gutters
Sidewalks	Concrete
Alley	Yes - paved
Rail	None
Lighting	Yes
Electric	Available – So. Cal Edison
Gas	Available – So. Cal Gas
Water	Available – Public municipality
Sewer	Available – Public municipality

Property Ratings

Access	Average
Street Frontage	Average
Shape	Average
Functional Utility	Fair - narrow small site
Visibility	Average
Drainage	Average
Adequacy of Utilities	Average
Traffic Pattern	Average

Entitlements / Future Development

Per public records information, the subject's site size is 5,355 square feet, with site dimensions of ± 45' along State Street and 119' along Church Street. There are no known entitlements currently being processed or approved for the site.

The city planning officials offered assistance in determining the likelihood of future development. According to officials at the planning department, any future development would likely require a street dedication of ± 4' in width along Church Street, new curb / gutter along Church Street, and the relocation of two above ground power poles along Church Street. **It is an extraordinary assumption of this report, that the subject site could be developed subject to the described street dedication and offsite improvements**.

The cost of the future offsites has been determined based on conversation with local contractors together with Marshall Valuation cost service:

Sidewalk: 480 SF x $15 PSF =	$9,600
Curb/Gutter: 120 LF x $30 PLF =	$4,800
Pavement & Street match =	$5,000
Relocate two electric power poles =	$40,000
Subtotal:	$59,400
Profit / Contingency of 10%:	$ 5,940
Total Cost of Offsites:	$65,340
Rounded to:	**$65,000**
PSF of the land:	**$12.14**

Frontage / Exposure / Access

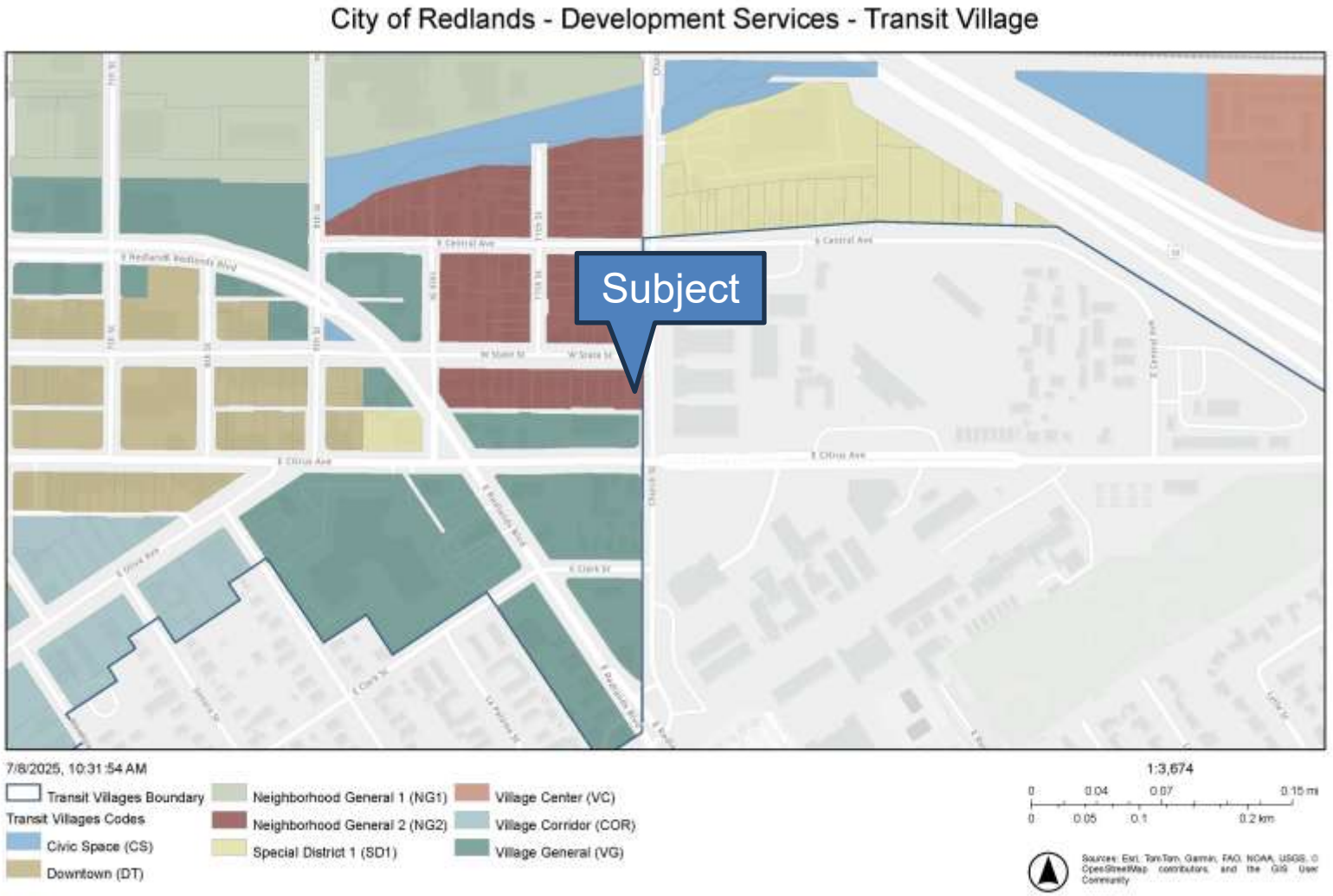
The subject property has ±119' of frontage on Church St., and 45' on E State St. Church St. is a two lane (one lane in each direction), The property is across the street from Redlands High School and adjacent Autozone. E State St. provides access to Historic Downtown Redlands. The freeway access is considered average to good with the Interstate 10 Freeway approximately 1 mile.

Zoning

According to the city planning department, the subject site is located in the Transit Village Specific Plan (SP65) with a land use designation of NG2 or Neighborhood General 2**.** The Neighborhood General 2 zone enables house-form buildings that accommodate residential and office uses. New buildings are up to two stories in height and are set back from the sidewalk behind front yards. Parking is located behind buildings. New buildings match or complement prevalent building setbacks along the length of the block and complement building heights and massing of adjacent buildings or buildings across the street.

Permitted uses include primarily administrative professional uses along with single-family residential and multi-family residential. Development standards are retained in file.
A complete zoning compliance survey has not been completed. However, based on a cursory review of the zoning ordinance, a residential use appears to be a compatible, conforming, and legal use of the site.

Zoning Map



Easements, Encroachments, and Restrictions

The appraiser was not provided with a preliminary title report to aid in the identification of easements, encroachments, or restrictions. Based on a visual inspection the property does not have any obvious adverse easements, encroachments, or restrictions that appear to impact the marketability of the property. The analysis assumes no adverse easements, encroachments, or restrictions.

Hazardous Substances

The appraiser was not provided with a Phase I or Phase II Environmental Assessment(s). Based on the visual inspection, the following has been noted:

- None

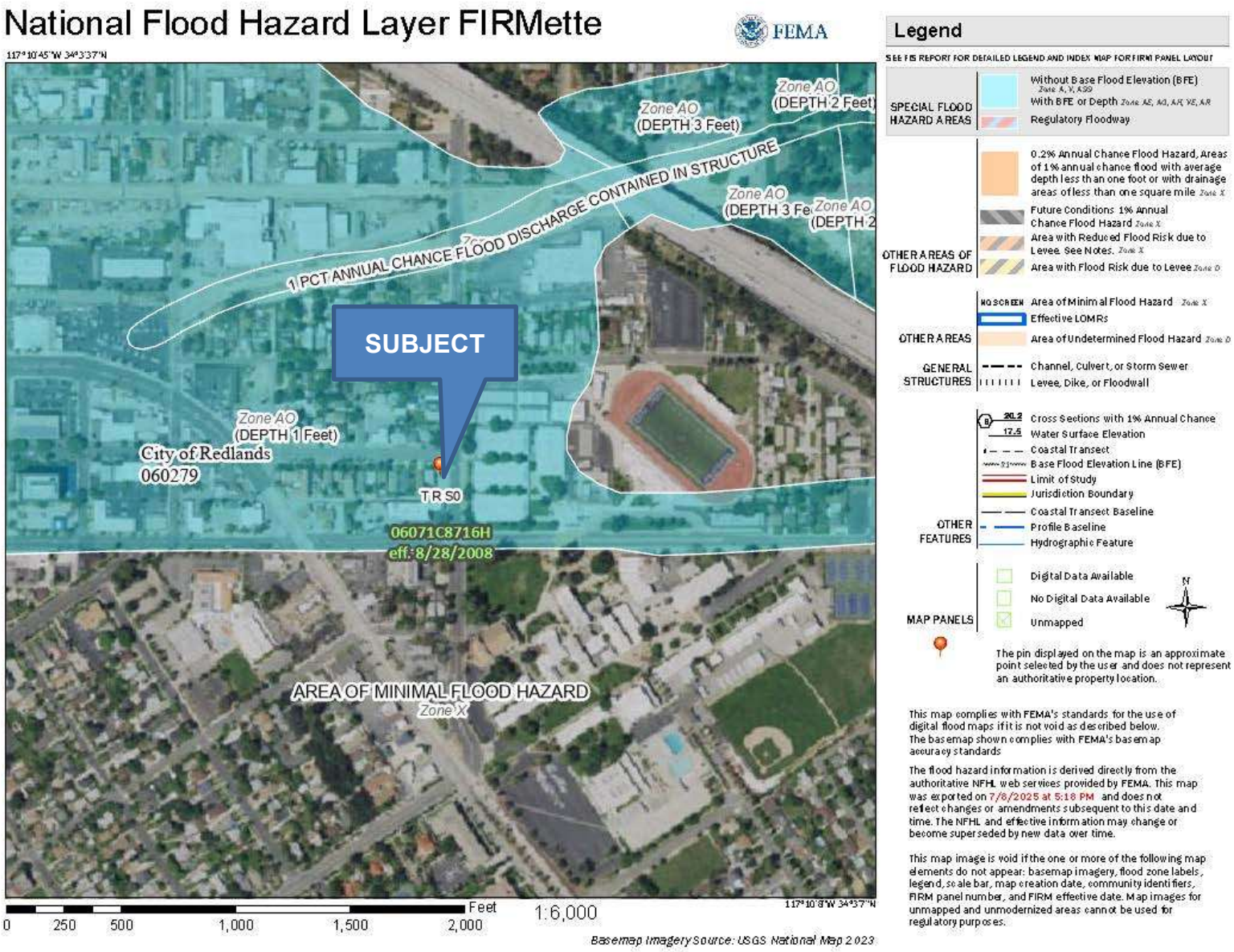
No underground fuel tanks are known to exist on or adjacent the site. There are no obvious spillage or significant staining from stored materials noted on site. Based on the cursory visual site inspection, the appraiser has assumed that the subject property is free from toxic and/or hazardous waste contamination.

Topography, Drainage and Soils

The subject site is relatively level and located near street grade. The appraiser is not an expert in the detection or analysis of soils problems. However, based on the visual inspection, there did not appear to be any obvious subsidence or other problematic soils conditions. The appraised value assumes the composition of the soil is adequate to support development of the site to its highest and best use.

Flood Zone

FLOOD MAP	
Source	FEMA
Flood Zone	AO
Description	1% annual chance of flood discharge
Map Panel	06071C8716H
Date	8/28/2008
Special Hazard Area	Yes
Participation	Regular / Eligible



Earthquake / Seismic Zones

The subject property is not within a California Alquist-Priolo Special Studies geographic hazard zone (i.e., an earthquake zone). However, the subject property is within five miles of at least two designated fault zones. Southern California is a maze of recorded fault zones. The subject's local area is not known to have any unusual reputation or suffer from any adverse impact associated with earthquakes.

Environmental Issues

The subject property is not covered with aquatic vegetation, nor is it located within close proximity of the ocean and is thus assumed to be out of any designated wetland area. In addition, the subject property is not known to be within a designated agricultural preserve or impacted by any government-protected species. The appraised value assumes the

subject site is unaffected by any environmental concern and can be developed to its highest and best use.

Entitlements

None

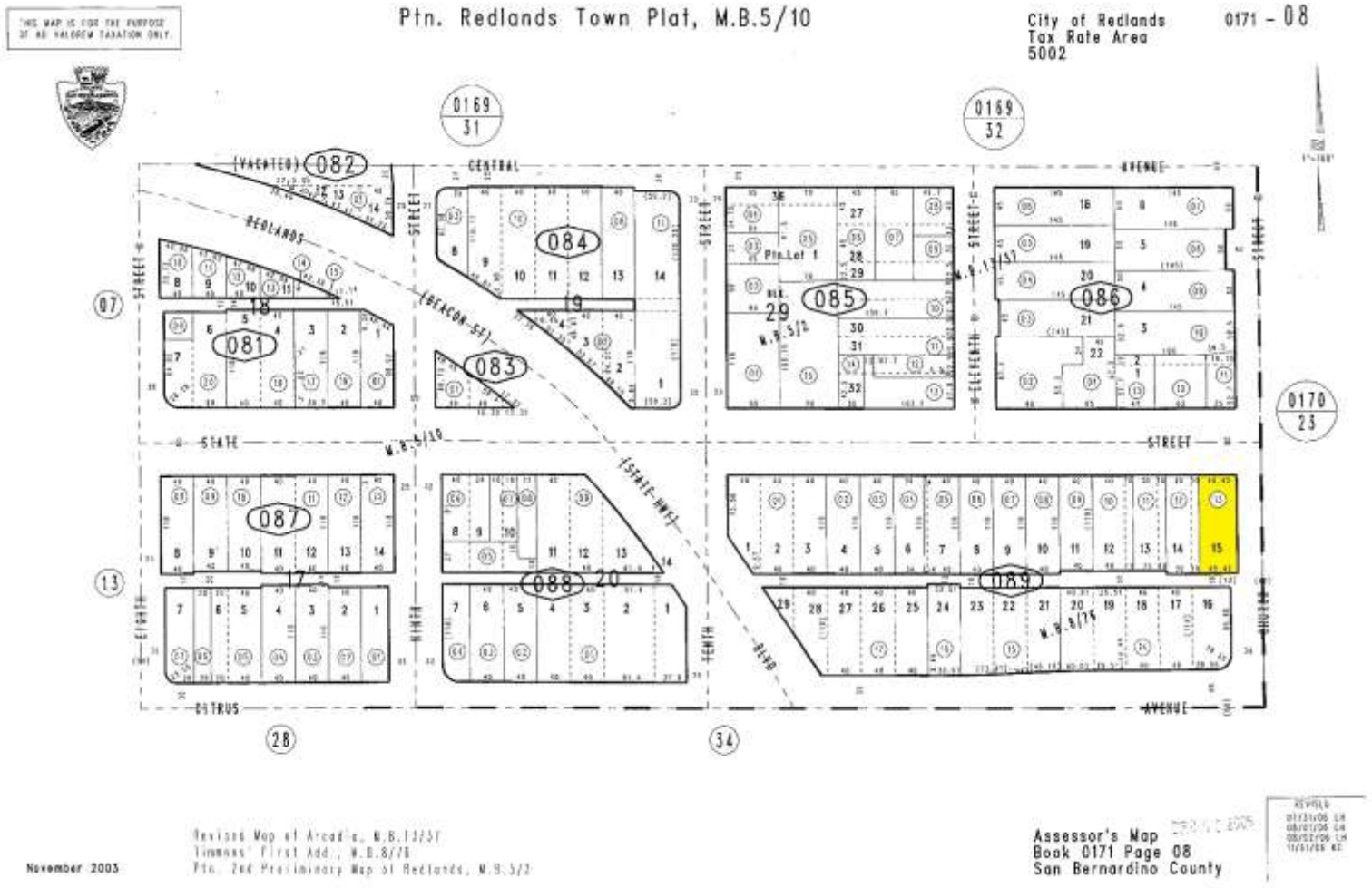
Structural Improvements

None.

Conclusions

Overall, the property benefits from its close proximity to Downtown Redlands. Given its location and size, the most likely use would be a small-lot residential development. The small size of the site will be made even more challenging with a potential street dedication and costs associated with offsite improvements, which includes the cost associated with relocating two electrical power poles.

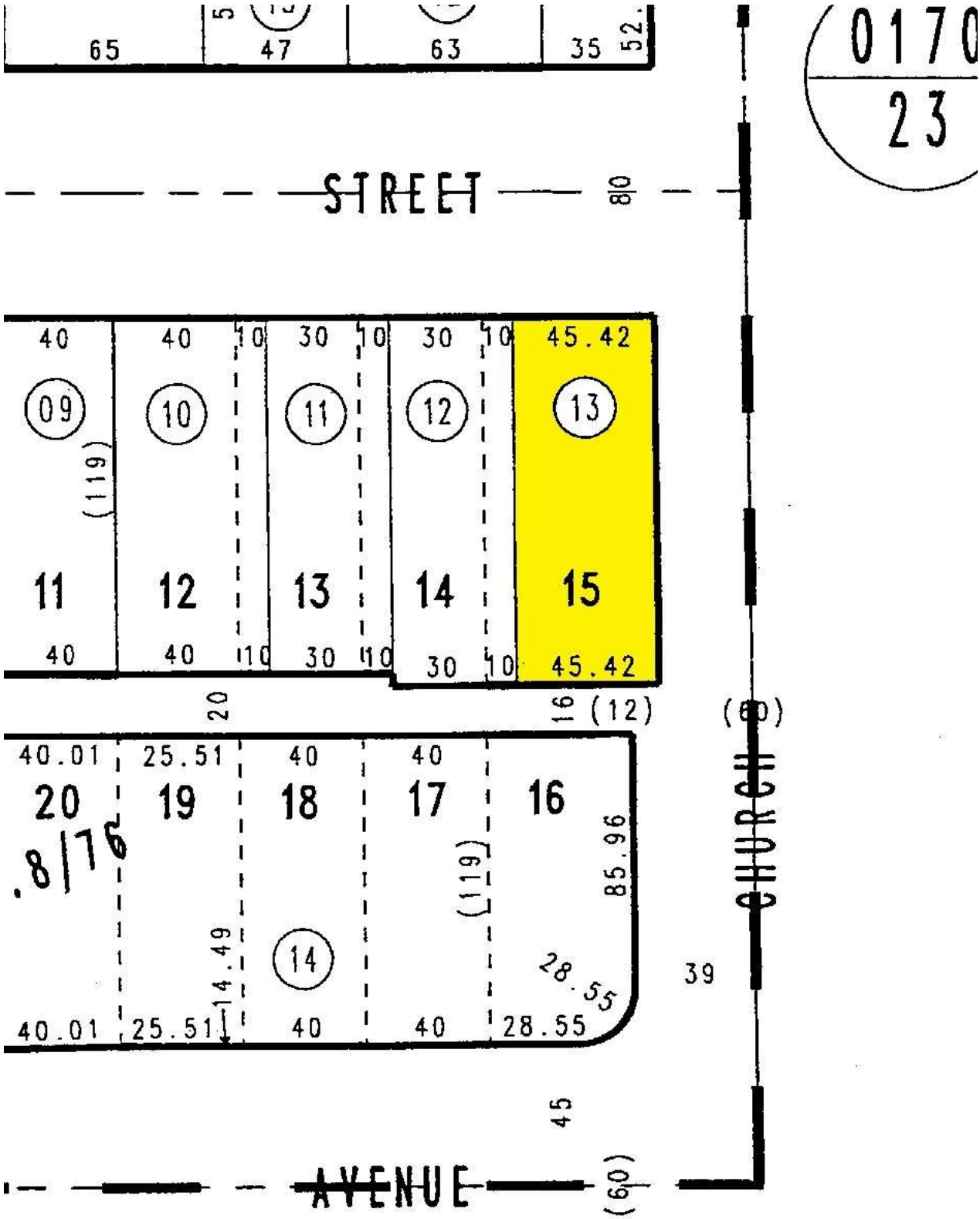
ASSESSOR'S PARCEL MAP



November 2003

Revised Map of Arcadia, M.B.13/37
Timmons' First Add., M.B.8/15
Ptn. 2nd Preliminary Map of Redlands, M.B.5/2

Assessor's Map
Book 0171 Page 08
San Bernardino County


0170
23
65
47
63
35
52.
STREET
80
40
40
10
30
10
30
10
45.42
09
10
11
12
13
(119)
11
12
13
14
15
40
40
10
30
10
30
10
45.42
20
16
(12)
(60)
40.01
25.51
40
40
20
19
18
17
16
.8/76
(119)
85.96
14.49
14
28.55
39
40.01
25.51
40
40
28.55
CHURCH
45
AVENUE
(60)

AERIAL VIEW

SUBJECT PHOTOGRAPHS

View of subject property from E. State St.

iew of subject property from Church St.

SUBJECT PHOTOGRAPHS

View of subject property from Alley

Alley

SUBJECT PHOTOGRAPHS

Looking West on E. State St.

Looking South on Church St.

HIGHEST AND BEST USE

Highest and Best Use is defined as:

"The reasonably probable and legal use of vacant land or improved property, which is physically possible, appropriately supported, financially feasible, and that results in the highest value."[4]

The determination essentially requires two analyses. The first determines the highest and best use "as-if vacant", while the second determines the highest and best use "as improved."

The first analysis of the site "as if vacant" requires some basic considerations as to what uses are reasonably possible, what uses are legally permitted with respect to zoning, deed restrictions, recorded covenants, conditions, and restrictions. In addition, the analysis must review the uses that are financially supported under existing and projected market conditions. The analysis must determine what uses among the alternatives are physically possible and will be the most profitable.

The second analysis "as-improved" involves much the same determinations as is required for the "as-if vacant" analysis, but must also consider the contributory value of the existing improvements.

As Vacant

- **Legally Permissible:** According to the city planning department, the subject site is located in the Transit Village Specific Plan (SP65) with a land use designation of NG2 or Neighborhood General 2**.** The Neighborhood General 2 zone enables house-form buildings that accommodate residential and office uses. New buildings are up to two stories in height and are set back from the sidewalk behind front yards. Parking is located behind buildings. New buildings match or complement prevalent building setbacks along the length of the block and complement building heights and massing of adjacent buildings or buildings across the street.

- **Physically Possible**: The property's physical size and shape are smaller than typical but are likely to be suitable for residential development. The site is generally level and positioned at or near street grade. Access to the site is adequate from publicly maintained streets and all typical utilities are available. Overall, the site is suitable for a small-lot residential use.

- **Financially Feasible**: As was presented previously in the Market Overview section of this report, high interest rates, the onset of inflation, are primary concerns of most market participants. Both rents and sales prices have generally plateaued over the 24 to 36 months. Price declines have been mitigated by the lack of available inventory. Market fundamentals would improve with a drop in interest rates. The increasing cost of construction has a negative impact on vacant land

[4] Ibid, Page 50

values and has reduced profitability. Financial feasibility is questionable under current economic conditions.

- **Maximally Productive**: Given the current volatility in the market, the maximally productive use is to hold for future small-lot residential construction. Any new construction should meet current market expectations with regard to construction amenities and should maximize site coverage according to zoning development standards.

Overall, the highest and best use as if vacant is to hold for future small lot residential development.

VALUATION

Market Value is the present worth of all expected future net benefits accruing from ownership of real estate. The appraisal process is a systematic, orderly and logical method of collecting, analyzing and processing market data in order to make an informed judgment of the Market Value of specific real property. In order to measure the present worth of future net benefits, three appraisal methods are typically developed for processing market data into indicators of value. They are: the ***Cost Approach***; the ***Sales Comparison Approach***; and the ***Income Approach.*** All three are Market Approaches. All three are interrelated because each is based on specific data collected from active participants in the real estate market. The applicability of each approach depends directly upon the nature of the market, which governs the quality and quantity of the data available.

Applicable Approaches for the Subject Property Valuation

For purposes of this analysis, the analysis has relied solely on the Sales Comparison Approach.

Both the Cost Approach and the Income Approach are excluded as the least applicable approaches to value.

Exclusion of the Cost Approach is based on:

- There are no structural improvements. Vacant land only.

Exclusion of the Income Approach is based on:

- The subject property appeals primarily to small developers rather than investors. Developers look to purchase similar land on a fee simple basis for construction purposes. This type of property is not typically purchased for its income generating capabilities.

DIRECT SALES COMPARISON APPROACH

The Direct Sales Comparison Approach involves directly comparing the subject property to similar properties that have recently sold or are listed for sale. The Direct Sales Comparison Approach is based upon the principal of substitution. This principal states that "… The value of a property that is replaceable in the market tends to be set by the cost of acquiring an equally desirable substitute property of similar utility and desirability within a reasonable amount of time."

A major premise of the Direct Sales Comparison Approach is that the market will determine a price for the subject property in much the same way that it determined the price of the comparable sales. Sales data similar in size, quality, and location to the subject were researched.

To determine the effect of time on the general level of sales prices, the sales were reviewed over a three-year period. The search consisted of a review of public records, published sources such as CoStar COMPS®, LoopNet®, AIR® Commercial Real Estate Association, local Multiple Listing Board, along with data and interviews provided directly by brokers and market participants active in the area.

A summary of comparable sales is located on the following page.

SUMMARY OF COMPARABLE DATA										
Data No.	Site Address City Assessor Parcel No.	Sale Date Doc. # Days On Market	Sales Price Property Rights Down Payment	Price PSF of Land	Land Area (NET) SF	Land Area Acres	Zoning	Flood Zone / Offsites	Comments	Buyer / Seller/Owner
SUB	21 Church St. Redlands, CA 92373 0171-089-13	Na Na	Na Fee Simple Cash Equivalent	NA	5,355	0.12	SP (NG2)	Flood zone AO Utilities available Part. Curb/Gutter	Corner site. Future development will likely require 4' street dedication, new curb/gutter/sidewalk, and relocating two power poles. Estimated cost is $65,000.	Na City of Redlands
	Verification: CRMLS, Public Records									
1	1024 6th St. Redlands, CA 92374 0169-081-05	2/12/2026 42263 2	$120,000 Fee Simple Cash	$18.69	6,419	0.15	R2	Flood Zone X Utilities available No curb or gutter	R-2 Multiple-Family Residential zoning allows for medium density multiple-family housing. Mid-block location.	Younis Loay Nn Redlands LLC
	Verification: CRMLS, Public Records									
2	28967, Greenspot Rd Highland, CA 92346 1210-201-56	3/10/2026 61828 27	$135,000 Fee Simple Cash	$21.10	6,398	0.15	EHV East Highland	Zone X Utilities available Curb/gutter	East Highland Village (EHV) District is intended as an area for small lot single-family residential detached housing with a maximum allowable density of six DUs per gross acre. The district further establishes a minimum parcel size of 5,000 square feet. Mid-block location. Long and narrow site.	Deans Services LLC Garcia Ibeth M & Cesar L
	Verification: CRMLS, Public Records									
3	2155 N. Pershing Avenue Sam Bernardino, CA 92405 0146-012-08	8/28/2025 208839 87	$138,000 Fee Simple Cash	$20.44	6,750	0.15	RS	Zone X Utilities available Curb/gutter	The RS zone is intended to promote the development of single-family detached units in a suburban setting with a minimum lot size of 7,200 SF. Previously developed site. Mid-block location.	Kemple James Residential Credit Opport
	Verification: CRMLS, Public Records									
4	25604 Walker AVE San Bernardino, CA 92404 0273-261-26	3/24/2026 74973 21	$50,000 Fee Simple Cash	$6.94	7,201	0.17	R-1	Zone X Utilities available None	Single-Family (R-1) District is intended for detached, single-family residential, small lot single-family detached, and mobile homes at a maximum allowable density of six DUs per gross acre. The district further establishes minimum parcel sizes of 7,200. Located at the end of a cul-de-sac and lacks offsite improvements. Surrounded by undeveloped land.	Rodriguez Victoria Milbes Juma J
	Verification: CRMLS, Public Records									
5	25604 Walker AVE San Bernardino, CA 92404 0273-261-26	n/a n/a 21	$60,000 Fee Simple Active Listing	$8.33	7,201	0.17	R-1	Zone X Utilities available None	Single-Family (R-1) District is intended for detached, single-family residential, small lot single-family detached, and mobile homes at a maximum allowable density of six DUs per gross acre. The district further establishes minimum parcel sizes of 7,200. Located at the end of a cul-de-sac and lacks offsite improvements. Surrounded by undeveloped land.	Rodriguez Victoria
	Verification: CRMLS, Public Records									

SALE DATA NO. 1

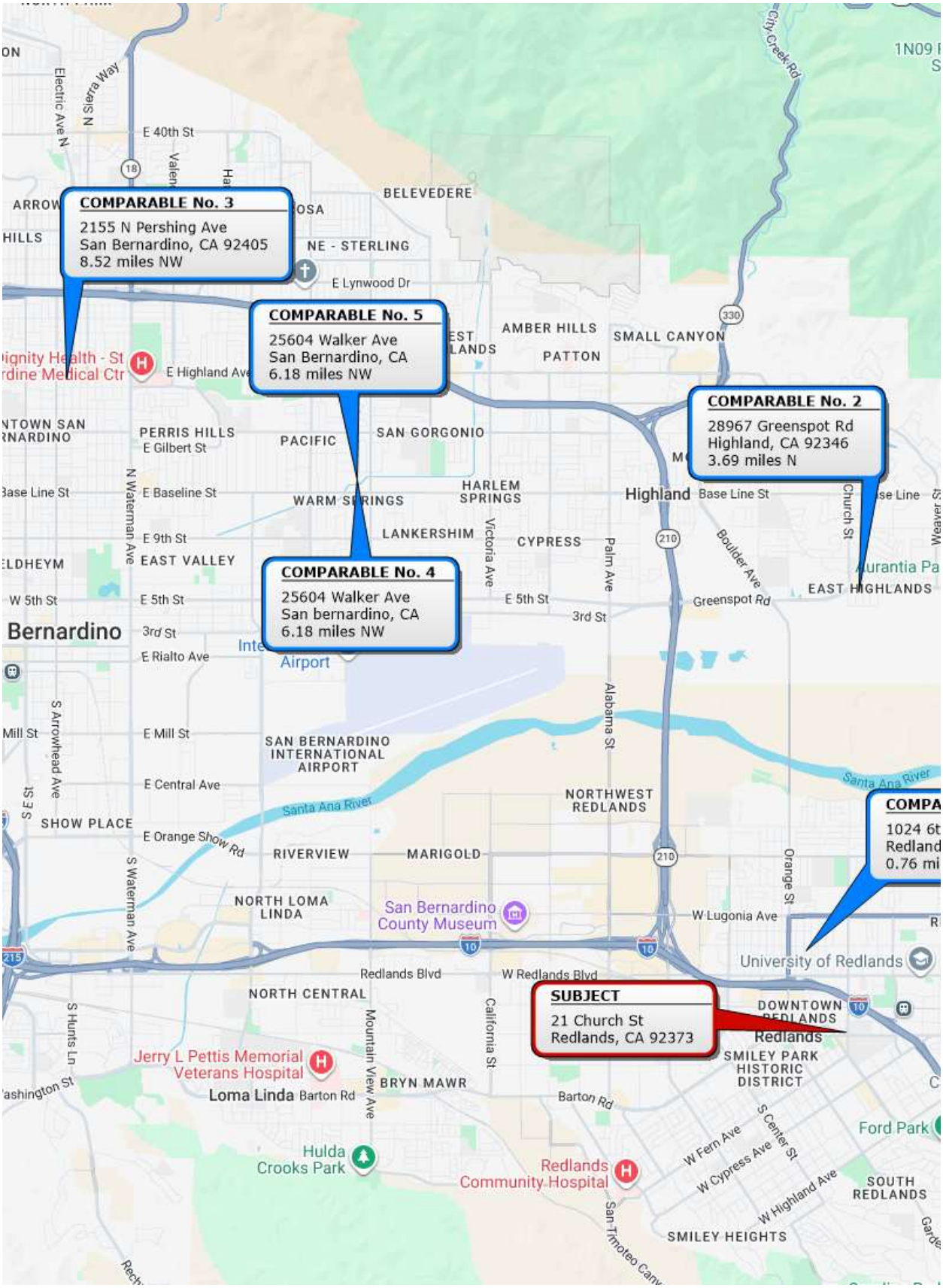
SALE DATA NO. 2

SALE DATA NO. 3

SALE DATA NO. 4

SALE DATA NO. 5

COMPARABLE LOCATION MAP



VALUATION

In order to compare the properties with the subject, there must be a common unit of comparison. The primary unit of comparison that is utilized in the Direct Sales Comparison Approach is the price per square foot of the building.

The basic elements of comparison that have been considered within this analysis include:

Transactional adjustments

- Property rights conveyed
- Financing terms
- Conditions of sale
- Expenditures anticipated after sale
- Market conditions

Property Adjustments

- Location
- Physical characteristics
- Economic characteristics

Ideally, the appraiser would make adjustments based on a paired sales analysis between the comparable properties and the subject. However, due to the limitations of the comparable data and complexities of each property, paired adjustments are not always possible. Instead, the appraiser has made most adjustments based on a combination of the appraiser's experience in the market, coupled with interviews conducted with active market participants such as brokers, buyers, and sellers.

Cost of construction is also considered as a basis for certain adjustments. In most cases, the adjustments are not meant to be exact measurements but an attempt to bracket a reasonable range of conclusions from a typical market participant.

The comparable data used in the analysis represents the best data available. An emphasis was placed first on site size, location, zoning and use. The comparable data was chosen in an attempt to “bracket” the subject property to better support the conclusion of value.

Real Property Rights Conveyed

All the comparables utilized transferred the fee simple interest. No adjustment for property rights is warranted.

Financing Terms

All of the sales reflect cash or market financing and no adjustments are warranted.

Conditions of Sale / Economic Characteristics

None of the closed sales reported any unusual conditions of sale that warrant adjustment.

Land Data No.5 is an active listing, which warrants a downward adjustment for the anticipated negotiations between buyer and seller.

Expenditures after Purchase

Expenditures after purchase is an adjustment made to the comparables for any significant or unusual expenditure that impacted the purchase price such as items of deferred maintenance (i.e., a major roof repair), toxic or hazardous waste clean-up, curing functional obsolescence, lease-up costs to stabilized occupancy, etc.

None of the comparable sales utilized within the analysis reported any unusual expenditure and no adjustments are made.

Market Conditions (Time)

The sale data closed escrow between August 2025 and March 2026, with Land Data No.5 being an active listing.

MLS analytic data presented in the Market Overview section of the report supports that starting in late September 2022, the market exhibited signs of slowing due to interest rate increases and higher cost of capital. Construction costs have continued to increase and the volatility in the market has had a negative impact on land values. The oldest land sale occurred in August 2025 and based on a paired analysis but recognizing the analytical data provided by the MLS, no adjustment for time has been made to any of the closed sales.

Market Identity

The subject property is located in the City of Redlands. Land Data No.1 is located in Redlands and warrants no adjustment.

Land Data No.2 is located in nearby city of Highland. This location is deemed slightly inferior and warrants an upward adjustment.

Land Data No.3, No.4 / No.5 are located in nearby San Bernardino. San Bernardino has historically been considered an inferior market area in terms of sale prices of finished homes and lots. Upward adjustments are warranted.

Exposure/Access

Sales Data No.3, No.4 / No.5 are in less conforming locations when compared to the subject. Both warrant slight upward adjustments.

Sales Data No.1 and No.2 are generally similar to the subject and no adjustment is warranted.

Site Size

The comparable data range from 6,419 SF to 7,201 SF. No adjustments are warranted.

Zoning

The subject property is zoned SP which allows for both AP and residential development. The most likely use is that of a small lot residence. All five of the comparable properties would allow residential use. No adjustment is warranted.

Offsite Improvements

The subject property is currently improved with curb, gutters, and sidewalk in place. However, as was presented previously, City planning officials indicated that any future development would likely require a street dedication of ± 4' in width along Church Street, new curb / gutter along Church Street, and the relocation of two above ground power poles along Church Street. **It is an extraordinary assumption of this report, that the subject site could be developed subject to the described street dedication and offsite improvements**.

The cost of the future offsites has been determined based on conversation with local contractors together with Marshall Valuation cost service:

Sidewalk: 480 SF x $15 PSF =	$9,600
Curb/Gutter: 120 LF x $30 PLF =	$4,800
Pavement & Street match =	$5,000
Relocate two electric power poles =	$40,000
Subtotal:	$59,400
Profit / Contingency of 10%:	$ 5,940
Total Cost of Offsites:	$65,340
Rounded to:	**$65,000**
PSF of the land:	**$12.14**

The primary cost associated with development is associated with relocating the two electric power poles.

Sale Data No.1, No.2, and No.3 appear to be finished or nearly finished lots, which will not require street match or relocating power poles. As such, all three comparable properties are superior and their respective offsite costs associated with development will be significantly less compared to the subject's. Therefore, downward adjustments are required for each. The amount of the adjustment is significant and is based on costs but tempered downward from the total costs to recognize that the comparables too will likely require some level of offsite costs.

Sale Data No.4 / No.5 is located at the end of a cul-de-sac street and lacks offsite improvements in front of the property. Although no costs are known for the development, the site will require the extension o the street together with curb, gutter, and sidewalk. Overall, the level of needed offsite improvements is considered similar to the subject and no adjustment has been made.

Functional Utility

The subject property is narrow and small which reduces the site's overall utility and makes any future construction more difficult.

Sale Data No.1 though 5 all have slightly superior widths and depths. All warrant downward adjustments.

Flood Zone

The subject property is located in a flood zone AO, which increases the risk of flood and the cost of future insurance premiums. All of the sale comparables are in Zone X, which has no threat of flooding and are superior to the subject. All warrant downward adjustments.

Entitlements

The subject property has no entitlements in place associated with future construction. All five of the comparable properties are similarly unentitled lots. No adjustment is warranted.

Adjustment Summary

The adjustment analysis is summarized on the following page.

ADJUSTMENT GRID												
		SUBJECT	SALE DATA NO. 1		SALE DATA NO. 2		SALE DATA NO. 3		SALE DATA NO. 4		SALE DATA NO. 5	
		21 Church St. Redlands, CA 92373	1024 6th St. Redlands, CA 92374		28967, Greenspot Rd Highland, CA 92346		2155 N. Pershing Avenue Sam Bernardino, CA 92405		25604 Walker AVE San Bernardino, CA 92404		25604 Walker AVE San Bernardino, CA 92404	
TRANSACTIONAL	Sale Date	Na	2/12/2026		3/10/2026		8/28/2025		3/24/2026		n/a	
	Sale Price	Na	$120,000		$135,000		$138,000		$50,000		$60,000	
	Adjusted	Na	$120,000		$135,000		$138,000		$50,000		$60,000	
	Cash Equivalent											
	Sale Price											
	Per Sq.Ft.	Na		$18.69		$21.10		$20.44		$6.94		$8.33
	Property Rights	Fee Simple	Fee Simple	0.00%	Fee Simple	0.00%	Fee Simple	0.00%	Fee Simple	0.00%	Fee Simple	0.00%
	Adjusted											
	Price/Sq.Ft.			$18.69		$21.10		$20.44		$6.94		$8.33
	Conditions of Sale	Typical	Typical	0.00%	Typical	0.00%	Typical	0.00%	Typical	0.00%	Listing	-10.00%
	Adjusted											
	Price/Sq.Ft.			$18.69		$21.10		$20.44		$6.94		$7.50
	Expenditures After Sale	None	None	0.00%	None	0.00%	None	0.00%	None	0.00%	None	0.00%
	Adjusted											
	Price/Sq.Ft.			$18.69		$21.10		$20.44		$6.94		$7.50
	Time /											
	Market Conditions	Current	2/12/2026	0.00%	3/10/2026	0.00%	8/28/2025	0.00%	3/24/2026	0.00%	n/a	0.00%
	Adjusted											
	Price/Sq.Ft. of Land			$18.69		$21.10		$20.44		$6.94		$7.50
	Contributory Value											
	Building/Site Improvements	None	Similar	0.00%	Similar	0.00%	Similar	0.00%	Similar	0.00%	Similar	0.00%
	Adjusted											
	Price/Sq.Ft. of Land	N/A		$18.69		$21.10		$20.44		$6.94		$7.50
PROPERTY	Market Identity	Average	Similar	0.00%	Inferior	5.00%	Inferior	10.00%	Inferior	10.00%	Inferior	10.00%
	Exposure / Access	Average	Similar	0.00%	Similar	0.00%	Inferior	10.00%	Inferior	15.00%	Inferior	15.00%
	Acres	0.12	0.15		0.15		0.15		0.17		0.17	
	Lot Size - Sq. Ft.	5,355	6,419	0.00%	6,398	0.00%	6,750	0.00%	7,201	0.00%	7,201	0.00%
	Zoning	SP	R2	0.00%	EHV	0.00%	RS	0.00%	R-1	0.00%	R-1	0.00%
	Offsites	Needs Offsite Imp.	Superior	-50.00%	Superior	-40.00%	Superior	-50.00%	Similar	0.00%	Similar	0.00%
	Functional Utility	Narrow / small	Superior	-5.00%	Superior	-5.00%	Superior	-5.00%	Superior	-5.00%	Superior	-5.00%
	Flood Zone	AO	X	-2.50%	X	-2.50%	X	-2.50%	X	-2.50%	X	-2.50%
	Entitlements	None	None	0.00%	None	0.00%	None	0.00%	None	0.00%	None	0.00%
	Total Adjustment	N/A		-57.50%		-42.50%		-37.50%		17.50%		17.50%
	Adjusted Price / Sq.Ft.	**Na**		**$7.95**		**$12.13**		**$12.78**		**$8.16**		**$8.81**

RECONCILIATION AND CONCLUSION OF AS-IS VALUE

Three of the five comparables warrant substantial downward adjustments due primarily to the high cost of the subject's offsites. Overall, the comparable sales offer a general cross-section view of the immediate market and provide adequate support for the value conclusion.

Based on the investigation and analysis summarized herein, and subject to the assumptions and limiting conditions set forth in this report, our concluded **As-Is Market Value** of the **Fee Simple Interest** in the subject property, **as of August 13, 2026 is:**

$9.00 PSF x 5,355 SF = $48,150

$50,000 (rounded)

ESTIMATE OF MARKETING/ EXPOSURE TIME

The estimate of the exposure time for the subject is supported by examining exposure times of similar recent sales in the market area. The estimate of the exposure time for the subject is supported by examining exposure times of similar recent sales in the market area. The comparable sales presented previously within the Sales Comparison Approach exhibited the following exposure times:

Comp. 1	Comp. 2	Comp. 3	Comp. 4	Comp. 5
386	229	87	85	49

Based on these indications, together with conversations with active brokers in the market area, an ***Exposure Time*** **of 6 to 12 months** has been concluded for the subject property.

The conclusion of Marketing Time for the subject property is the estimate of time, going forward, that the property will require to achieve a sale. Most market participants agree that the marketing time going forward is expected to be similar to the trends set in the past 12 months due primarily to the continued sluggish economic and market conditions in the region. As such, the forecast of *Marketing Time* for the subject property is concluded to be similar to the previously concluded *Exposure Time*.

Based on the local market data, a ***Marketing Time*** **of 6 to 12 months** has been concluded for the subject property.

CERTIFICATION OF APPRAISAL

I, James G. Towers certify that, to the best of my knowledge and belief:

1. The statements of fact contained in the appraisal report, upon which the analysis, opinions, and conclusions expressed herein are based, are true and correct.
2. The reported analysis, opinions and conclusions are limited only by the reported assumptions and limiting conditions, and is my personal, impartial, and unbiased professional analysis, opinions and conclusions.
3. I have no present or prospective interest in the property that is the subject of this report, and I have no personal interest or bias with respect to the parties involved.
4. I have no bias with respect to the property that is the subject of this report or to the parties involved with this assignment.
5. My engagement in this assignment was not contingent upon developing or reporting predetermined results.
6. My compensation for completing this assignment is not contingent upon the development or reporting of a predetermined value or direction in value that favors the cause of the client, the amount of the value opinion, the attainment of a stipulated result, or the occurrence of a subsequent event directly related to the intended use of this appraisal.
7. My analysis, opinions, and conclusions were developed, and this report has been prepared, in conformity with the requirements of the Uniform Standards of Professional Appraisal Practice.
8. I have made a personal inspection of the property that is the subject of this report.
9. Digital photography presented in this report has not been altered in any way that would mislead the reader.
10. I did not base, either partially or completely, my analysis and/or the estimate of value on the race, color, religion, sex, handicap, familial status, health, or national origin of either the present or prospective owners, occupants, or users of the subject property or of the present or prospective owners, occupants, or users of the properties in the vicinity of the subject property.
11. I am competent to perform this appraisal assignment, by virtue of previous experience with similar assignments and/or proper research and education as to the specific property type being appraised.
12. This appraisal assignment was not based on a requested minimum valuation, a specific valuation, or the approval of a loan.
13. Ryan Towers (CA#3014518) has provided professional assistance in this appraisal assignment. Involvement in the appraisal assignment includes, but is not limited to, the identification and inspection of the subject property and comparable data, research into the physical and economic factors affecting the subject property, data research, and the analyses applied to arrive at the opinions and conclusions herein. James Towers signs the certification in each report as principal appraiser, acknowledges the contributions of Ryan Towers in the certification (Standards Rule 2-3), and takes full responsibility for the contents of the report (Standards Rule 2-2(a) (vii), (b) (vii), or (c) (vii), as applicable).
14. I **have not** performed a prior appraisal(s) or other service that involved the subject property during the three-year period immediately preceding the agreement to perform this assignment.
15. I certify that, to the best of my knowledge and belief, the reported analysis, opinions and conclusions were developed, and this report has been prepared, in conformity with the requirements of the Code of Professional Ethics and the Standards of Professional Appraisal Practice of the Appraisal Institute.
16. I certify that the use of this report is subject to the requirements of the Appraisal Institute relating to review by its duly authorized representatives.
17. This appraisal is intended to comply with the OCC's amended Appraisal Rule, effective June 7, 1994, as published in the Federal Register, Volume 59, No. 108, and with the Interagency Appraisal and Evaluation Guidelines, dated December 10, 2010.
18. As of the date of this report, I James G. Towers have completed the continuing education program for Designated Members of the Appraisal Institute.

By: August 23, 2026

James G. Towers, MAI, AI-GRS, CCIM, CA BREA Certification #AG003282 Date

QUALIFICATIONS OF APPRAISER – JAMES G. TOWERS, MAI, AI-GRS, CCIM

I James G. Towers am self-employed and doing business as Towers & Associates, a full-service real estate appraisal and consulting firm. I specialize in the completion of narrative as well as approved form appraisals of all types of commercial, industrial, and residential properties. I have extensive experience in appraisal and consulting projects ranging from single-family residential homes to investment-grade office buildings, shopping centers, industrial buildings, business parks, apartment buildings / complexes, residential subdivisions, and master-planned communities. Appraisals have been performed throughout Southern California on performing and non-performing real estate at various stages of development.

My primary geographical area for single-family, small residential income and small commercial/industrial properties is typically confined to the Inland Empire (Riverside and San Bernardino Counties). Larger investment grade properties are appraised throughout Riverside, San Bernardino, Los Angeles, and Orange Counties.

PROFESSIONAL DESIGNATIONS AND AFFILIATIONS

California Certified General Appraiser – BREA Appraiser Identification Number AG003282. Expiration Date is June 7, 2028.

Designated Member of the Appraisal Institute (MAI & AI-GRS); Account # 102341

Designated Member of the CCIM Institute (CCIM); Pin #: 23927

California Licensed Real Estate Broker – DRE Identification Number 01342640

EXPERIENCE

TOWERS & ASSOCIATES – Redlands, California
Self-Employed Real Estate Appraiser and Consultant
January 1994 to present

WELLS FARGO BANK – Los Angeles, California
Review Appraiser - Real Estate Technical Services
May 1992 to January 1994

SECURITY PACIFIC BANK / BANK OF AMERICA – Riverside, California
Assistant Vice President – Riverside Commercial Appraisal
November 1989 to May 1992

TOWERS APPRAISAL SERVICE – Beaumont, California
Self-Employed Real Estate Appraiser and Consultant
March 1986 to November 1989

TOWERS APPRAISAL SERVICE – Beaumont, California
Staff Appraiser
February 1982 to March 1986

EDUCATION

CALIFORNIA STATE UNIVERSITY – San Bernardino, California
Graduated 1988, with Bachelor of Arts degree, Business Administration with a concentration in Economics

Appraiser Qualifications Continued

SUCCESSFULLY COMPLETED PROFESSIONAL COURSES

Course	Provider
Real Estate Appraisal Principles	AIREA
Residential Valuation	AIREA
Capitalization Theory and Techniques Part A	AIREA
Capitalization Theory and Techniques Part B	AIREA
Case Studies in Real Estate Valuation Analysis	AIREA
Standards of Professional Practice	Appraisal Institute
Report Writing and Valuation Analysis	Appraisal Institute
Condemnation Appraising – 710	Appraisal Institute
Real Estate Appraisal X463	University of California Riverside
Real Estate Principles	Mt. San Jacinto College
Real Estate Practice	Anthony Schools
Real Estate Legal Aspects	Anthony Schools
Tools & Techniques for Managing an Appraisal Practice	McKissock
National USPAP Update	Appraisal Institute
California Laws & Regulations	McKissock
Appraising the Oddball	McKissock
Fair Housing	McKissock
Relocation	McKissock
Technology for Today's Appraiser	McKissock
The Cost Approach	McKissock
Business Practices and Ethics	Appraisal Institute
Advanced Sales Comparison & Cost Approach	Appraisal Institute
Advanced Market Analysis and Highest & Best Use	Appraisal Institute
Review Theory – General	Appraisal Institute
Financial Analysis for Commercial Investment RE	CCIM Institute
Market Analysis for Commercial Investment RE	CCIM Institute
User Decision Analysis for Commercial Investment RE	CCIM Institute
Investment Analysis for Commercial Investment RE	CCIM Institute
Preparing to Negotiate	CCIM Institute
Ethics 2020	CCIM Institute

PARTIAL LIST OF CLIENTS PREVIOUSLY SERVED

- Wells Fargo Bank
- Bank of the West
- Citizens Business Bank
- Hanmi Bank
- U.S. Bank
- Bank of America
- City National Bank
- Union Bank
- Provident Savings Bank
- Citibank
- First Security Bank
- Chase Bank
- California Federal Bank
- Commercial Capital Bank
- Manufacturers Bank
- Inland Valley Credit Union
- Arrowhead Credit Union
- American Business Bank
- Banc of California

ADDENDUM

Engagement Letter
Appraiser's License

Towers & Associates
James G. Towers, MAI, AI-GRS, CCIM
P.O. Box 7783
Redlands, CA 92375
Office: 909-335-1735
Direct / Mobile: 909-223-9328
E-Mail: jtowers@live.com

July 31, 2026

Proposal and Appraisal Contract for Services

City of Redlands
C/o: Ms. Trish Munoz, MBA
Interim FCS Manager
Facilities & Community Services
35 Cajon St. Suite 222
Redlands, CA 92373
909-848-6605
tmunoz@cityofredlands.org

RE: Appraisal Assignment

Dear Ms. Munoz,

Towers & Associates is pleased to submit this Proposal and Terms for this assignment.

PROPOSED APPRAISAL ASSIGNMENT:

Client:	City o Redlands c/o Ms. Trish Munoz Transmitted Via Email
Current Owner:	City of Redlands
Property Identification:	Vacant Residential Land APN: 0171-089-13-000 Located at the SW Corner of Church Street and E. State St. Redlands, CA 92374
Requested Date of Value:	Current
Property Rights Appraised:	Fee Simple
Purpose of Appraisal:	To determine Market Value.
Intended Use:	Exclusive use of the client to update prior report and for potential sale purposes.
Intended Users:	City of Redlands (Client"), the client's agents, successors and / or assigns, and other such parties and entities (if any) expressly recognized.

BID INFORMATION:

Total Fee:	**$2,000**
Payment:	Payment is due upon completion of report
Completion Date:	Approximately 3 weeks from engagement
Delivery Instructions:	Electronic delivery in Adobe PDF file format
Report Type:	Complete Appraisal
Format:	Narrative
Date Submitted:	7/31/2026
Requested By:	Ms. Trish Munoz
Voice:	909-848-6605
Email:	tmunoz@cityofredlands.org

SUBMITTED BY:

Towers & Associates
James G. Towers, MAI, AI-GRS, CCIM
P.O. Box 7783
Redlands, CA 92375
Office:(909) 335-1735
Direct: (909) 223-9328
E-Mail: jtowers@live.com

TERMS OF ENGAGEMENT

1. Fee and Payment Terms

   The total fee for this appraisal assignment is payable upon delivery of report. This fee is based solely on the scope of work outlined in this letter and does not include court testimony, depositions, or any other legal proceedings. Should court-related services be required, they will be billed at an additional rate to be agreed upon in a separate agreement.

2. Limitation of Liability

   a. The appraisal report is prepared solely for the intended use and intended users identified in this letter. No third-party reliance is permitted.

   b. This appraisal is subject to the assumptions and limiting conditions to be outlined in the final report.

3. Confidentiality

   All information provided to Towers & Associates will be treated as confidential and used exclusively for the purposes of this assignment, except as required by law or professional standards.

4. Scope of Work

   Appraisal to be prepared under the reporting requirements set forth in Standards Rule 2-2(a) of the Uniform Standards of Professional Appraisal Practice (USPAP). The report to include discussions of the data, reasoning, and analysis that were used to develop the opinion of value. It also includes descriptions of the subject property, the property's locale, the market for the property type, and the appraiser's opinion of highest and best use. Any data and analysis not

presented in the summary appraisal report can be obtained from the appraiser's work file(s) upon request.

Prior to accepting this assignment, the appraiser and client have together identified the appraisal problem to be addressed as being the determination of:

Market Value. Fee Simple Interest Appraised

In compliance with the Competency Rule of USPAP, this appraiser has the knowledge and experience to complete the assignment competently.

The subject property to be visually inspected personally by James Towers along with its environs and relevant market data. The appraiser's inspection of the subject property typically involves the following:

- The inspection of the subject property will be visual in nature, without the use of any specialized equipment.
- The inspection of comparable data is typically limited to what can be visually observed from the public street and / or historical satellite imaging.
- The effective date of the Market Value will reflect the most recent date of physical inspection.
- The subject's site area to be determined from the assessor's parcel map and / or other client provided documentation.
- Building (if any) and site specifications determined from the onsite visual inspection and documentation provided by the client.
- Public sources have been utilized to determine the property's historical zoning and/or to confirm the status of any changes to the zoning.

This appraisal will include all appropriate and necessary approaches to value. Those approaches will include at minimum the following:

- **Sales Comparison Approach**

Existing lease contract(s) and any other encumbrances affecting the subject's value and/or marketability to be analyzed in arriving at the concluded estimate(s) of the current market value of the identified property rights, as appraised under the stated valuation premise(s).

The market data collected, evaluated, and analyzed in the valuation of the subject property will include sales data, construction cost data (if any), market rental information (if any including rates, terms, etc.), market expense data (if any), as applicable. Market trends, including the supply of, and demand for, competing properties of this type in the subject's market area to be analyzed. All data has been obtained from sources that the appraiser deems reliable. Where possible and practical, the data will be verified with more than one source including the principals and/or agents involved in the transaction. Public records may also have been used as a source of verification.

This appraisal is intended to comply fully with:

- The current Uniform Standards of Professional Appraisal Practice ("USPAP") promulgated by the Appraisal Standards Board of the Appraisal Foundation;
- Appraisal Institute Standards of Professional Appraisal Practice;

Legal testimony or other related legal proceedings are not a part of this appraisal assignment.

5. Acceptance

By signing below, you agree to the terms outlined in this letter of engagement. Upon receipt of this signed letter and the retainer payment, Towers & Associates will schedule the inspection and commence work.

ACCEPTANCE OF PROPOSAL

Per your request, I am submitting this engagement letter to retain my services as an appraiser. When executed and delivered by all parties, this letter of engagement serves as the Agreement for appraisal services by and between Towers & Associates and Client.

Please review, sign, and return by e-mail or mail. Your signature authorizes Towers & Associates to complete the assignment.

Regards,

James G. Towers, MAI, AI-GRS, CCIM
BREA # AG003282; Expires 6/07/2028
Towers & Associates

Signature

July 21, 2026
Acceptance Date:

Tricia Munoz
Name

Interim FCS Manager
Title

909-848-6605
Phone Number

tmunoz@cityofredlands.org
E-Mail Address

Business, Consumer Services & Housing Agency

BUREAU OF REAL ESTATE APPRAISERS
REAL ESTATE APPRAISER LICENSE

James G. Towers

has successfully met the requirements for a license as a residential and commercial real estate appraiser in the State of California and is, therefore, entitled to use the title:

"Certified General Real Estate Appraiser"

This license has been issued in accordance with the provisions of the Real Estate Appraisers' Licensing and Certification Law.

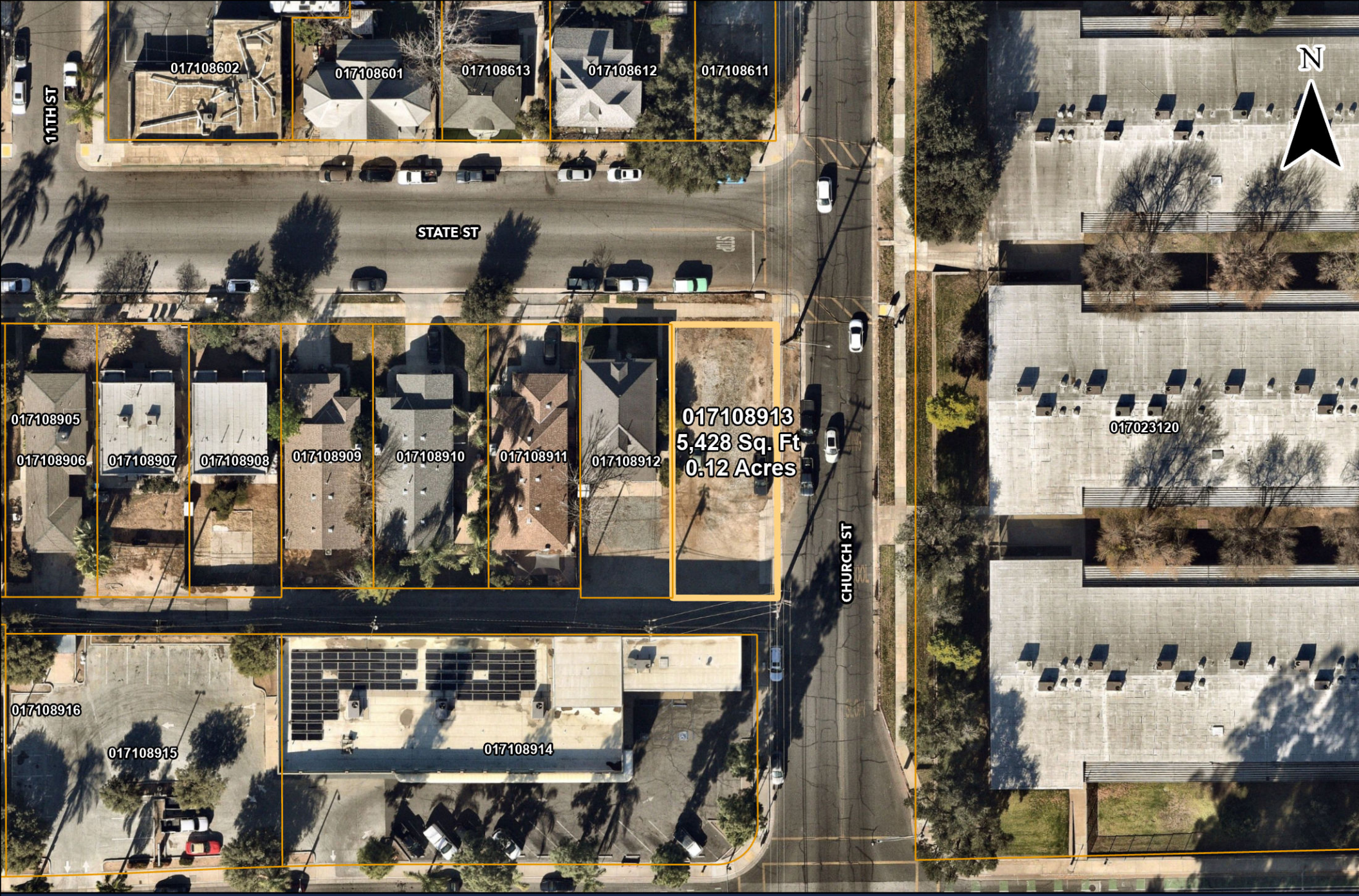
BREA APPRAISER IDENTIFICATION NUMBER: AG 003282

Effective Date: June 8, 2026
Date Expires: June 7, 2028

Angela Jemmott, Bureau Chief, BREA

3086674

THIS DOCUMENT CONTAINS A TRUE WATERMARK - HOLD UP TO LIGHT TO SEE "CHAIN LINK"



APN 0171-089-13

21 N Church Street

Parcel boundaries

0 50 100 Feet

City of Redlands
***Author:** Redlands GIS*
Date: 4/28/25

03/13/25

Chris Boatman, Assistant City Manager
City Of Redlands

Offer to Purchase 21 Church St, Redlands CA 92374

Dear Mr. Boatman,

I am writing to submit an offer of $10,000 to purchase the property located at 21 Church St.

My intent is to save the home at 616 E State St from demolition. Below is a historic picture of two homes; the right home is 616 E State St.

The owner of 616 E State St is willing to let the home be moved to 21 Church St, and I have confirmed with Redlands Chief Building Official John Thompson that the lot is suitable for the historic structure. Thank you for helping save a piece of our heritage.

Thank you for your time and consideration,

Zach Smith

RESOLUTION NO. 1744

A RESOLUTION OF THE PLANNING COMMISSION OF THE CITY OF REDLANDS FINDING THAT THE POTENTIAL SALE OF REAL PROPERTY BY THE CITY OF REDLANDS, FOR ONE PARCEL LOCATED AT THE SOUTHWEST CORNER OF STATE STREET AND CHURCH STREET (APN: 0171-089-13-0000) WOULD BE IN CONFORMITY WITH THE REDLANDS GENERAL PLAN.

WHEREAS, property owner City of Redlands wishes to sell certain real property located at 21 North Church Street (APN: 0171-089-13-0000), currently vacant and unimproved; and

WHEREAS, the subject property (APN: 0171-089-13-0000) is a total of approximately 5,355 square feet (or 0.12 acre) and is designated as "Transit Village" on the 2035 General Plan Land Use Map; and

WHEREAS, prior to sale or acquisition of real property by a local agency, California Government Code Section 65402 requires a finding of General Plan conformity by the Planning Commission as to the location, purpose, and extent of such sale or acquisition; and

WHEREAS, on March 10, 2026, the Planning Commission held a public meeting and considered the staff report, oral report, the testimony, and the written evidence submitted by and on behalf of the applicant concerning a General Plan conformity finding for the subject property; and

WHEREAS, a determination of General Plan conformity is exempt from review under the California Environmental Quality Act ("CEQA") pursuant to CEQA Guidelines Section 15061(b)(3) which provides that CEQA applies only to projects which have the potential for causing a significant effect on the environment. There is no possibility that this determination may have a significant effect on the environment. Any future development proposed on the subject property will be subject to CEQA.

NOW, THEREFORE, BE IT RESOLVED BY THE PLANNING COMMISSION OF THE CITY OF REDLANDS AS FOLLOWS:

SECTION 1. CALIFORNIA ENVIRONMENTAL QUALITY ACT. The determination of General Plan conformity for the sale of Assessor's Parcel No. 0171-089-13-0000 is exempt from environmental review in accordance with CEQA Guidelines Section 15061(b)(3), as there is no possibility of significant environmental effects from the sale of real property.

SECTION 2. FINDING OF GENERAL PLAN CONFORMITY. The Planning Commission hereby finds that the sale of 21 N. Church Street (Assessor's Parcel No. 0171-089-13-0000) is in conformity with Redlands General Plan.

SECTION 3. EFFECTIVE DATE. This Resolution shall become effective upon adoption.

ADOPTED, SIGNED AND APPROVED this 10th day of March, 2026.

Karah Shaw, Chair
Planning Commission

ATTEST:

Katherine Coleson, Secretary to the Planning Commission

I, Katherine Coleson, Secretary to the Planning Commission of the City of Redlands, hereby certify that the foregoing resolution was duly adopted by the Planning Commission at a regular meeting thereof held on the 10th day of March, 2026, by the following vote:

AYES: 7
NOES: 0
ABSENT: 0
ABSTAIN: 0

Katherine Coleson,
Secretary to the Planning Commission

City Council **AGENDA ITEM NO. M1.**

DATE: October 6, 2026

TO: Honorable Mayor and City Council Members

SUBJECT: Individual Council Member Report on Activities for September 2026 from Mayor Pro Tem Shaw (City Clerk Donaldson)

DISCUSSION:

Mayor Pro Tem Shaw has requested to include this report on the agenda for recording purposes. The report does not require City Council approval.

Attachments

September_2026_Council_Activities.pdf

September 2026 Council Activities

Mayor Pro Tem Marc Shaw

- Attended Redlands Chamber of Commerce Rise and Shine
- Spoke at Plymouth Village regarding city events and developments
- Attended the League of Cities Annual Conference in Anaheim as the City's Voting Delegate
- Attended the CONFIRE Board of Directors meeting
- Met with consultants working on City Manager and City Attorney performance evaluations
- Meeting with City Manager to discuss ongoing issues