Contract # AR2477

STATE OF UTAH COOPERATIVE CONTRACT

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

Cisco Systems, Inc.
Name
170 West Tasman Drive
Address
San Jose CA 95134
City State Zip

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

Contact Person Mimi Nguyen-Farr Phone #408-527-2627 Email mimnguye@cisco.com
Vendor #VC0000118462 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: 09/30/2016 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: Contractor's Service Documents
ATTACHMENT F: Contractor's Service Description and Contractor's Supplemental End User License Agreement
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

November 11, 2016
Contractor's signature Date

Phil Lozano
Director, Finance
Type or Print Name and Title

STATE

11.14.2016
for Director, Division of Purchasing Date

APPROVED BY LEGAL

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

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 ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits to the Master Agreement, as negotiated and executed by the parties;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Purchase Order or Statement of Work (including 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 agreed by the parties 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.

Applicable Laws means local, state or federal laws or regulations, to the extent applicable to the relevant Services provided by Contractor, including, but not limited to such laws and regulations regarding data privacy and security.

Cloud Equipment means the collective Contractor components owned and used by Cloud Provider to provide the Cloud Services to Purchasing Entity and any other monitoring tools, testing tools, and administration and management tools used for delivery of the Cloud Services.

Cloud Provider shall mean Contractor or CMSP Partner, as applicable.

Cloud Provider Sites means premises that are owned, controlled, or occupied by Cloud Provider and used by Cloud Provider for provision of the Cloud Services;

CMSP Partner means a Contractor's Authorized Fulfillment Partner as approved by the Lead State.

CMSP Services shall mean in scope offerings which may be provided by a CMSP Partner, which are running on Contractor-powered infrastructure and based on Contractor recommended and validated architectures. As such CMSP Service offerings become available, the parties may add such offerings by amending the Agreement as mutually agreed upon by Contractor and Lead State. Additional terms regarding the provision of the CMSP Services are set forth on Attachment E to this Agreement.

Contractor Cloud Services shall mean cloud-enabled "X as a Service" ("XaaS") offerings made available by Contractor or one of Contractor's affiliates under this Agreement, and which are currently on Contractor's Global Price List, such as Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"), as well as other cloud-related offerings. Additional terms regarding the provision of the Contractor Cloud Services are set forth on Attachment E to this Agreement.

Confidential Information means proprietary and confidential Information received by Contractor or Purchasing Entity in connection with the Agreement and their relationship. Such Confidential Information may include, but is not limited to, trade secrets, know how, inventions, techniques, processes, programs, schematics, Software, source code documents, data, customer lists, personnel records, financial information, and sales and marketing plans, or any other information which the receiving party knows or has reason to know is confidential, proprietary, or trade secret information of the disclosing party, as well as, in the case of Contractor, any information posted on Contractor's website.

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 Master Agreement.

Data Breach means any actual non-authorized access to or acquisition of computerized Non-Public Data or Purchasing Entity Data that materially compromises the security, confidentiality, or integrity of the Non-Public Data or Purchasing Entity Data, or the ability of Purchasing Entity to access the Non-Public Data or Purchasing Entity Data. A Data Breach also includes a major security breach to the Contractor's system, regardless of whether Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data**.**

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

Data Center means the Contractor data center housing the servers and other equipment necessary to provide the basic functionality of the Cloud Services, as described in the applicable service description. Other data centers used to store records regarding maintenance and support (even where such records contain Purchasing Entity's Data), shall not be considered Data Centers.

Data Collection Tools mean hardware or Software tools that support Contractor's ability to provide troubleshooting on critical cases, data analysis, and report-generation capabilities.

Documentation means user manuals, training materials, service descriptions and specifications, technical manuals, license agreements, supporting materials, and other information relating to Services offered by Contractor, whether distributed in print, electronic, CD-ROM, or video format.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, except as otherwise noted in the applicable Contractor documentation, including but not limited to viruses, worms, 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 (except for the expiration of a subscription based service), 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"). This type of data includes, but is not limited to: Purchasing Entity's Data, Personally Identifiable Health Information, and Protected Health Information.

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined as 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 Rights means any and all proprietary rights, in tangible or intangible form, and all rights, title, and interest therein, including (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms, and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

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, and other terms and conditions.

Participating Entity means a state, or other legal entity, which is 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.

Purchasing Entity Data means data alone or in combination, that is the output of any computer processing or other electronic manipulation, or otherwise created in the course of Purchasing Entity's use of the Services provided under this Agreement, 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. Purchasing Entity Data does not include data generated by Data Collection Tools.

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 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.

Price List means the then current Contractor global price list for the Services.

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. PHI does not include network centric information such as IP addresses or MAC addresses.

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 and/or Statement of Work against the Master Agreement and becomes financially committed to the purchase.

Purchasing Entity Site means premises that are owned, controlled, or occupied by Purchasing Entity that are made available for use by Cloud Provider or its subcontractors for provision of the Cloud Services.

Purchase Order or Order means a written or electronic order from Customer to Contractor for the Services to be provided under this Agreement.

Service Description or Offer Description means the documentation, which describes and governs the provision of the Cloud Services, which for Contractor Cloud Services will be identified and attached to the applicable Purchase Order, or for Contractor Cloud Services that are sold via Fulfilment Partners, will be attached to the Fulfilment partner's quote for Contractor Cloud Services. Service Descriptions are available for informational purposes online at http://www.cisco.com/go/servicedescriptions/.

Services or Cloud Services mean any of the Contractor Cloud Services and/or CMSP Services, including their specifications described in the accompanying Services Description, ordered under a Purchase Order and/or Statement of Work (SOW) referencing this Agreement, and supplied or created by the Contractor pursuant to this Master Agreement and the terms on Attachment E.

Security Incident means the possible unauthorized access to a Purchasing Entity's Non-Public Data and/or Purchasing Entity Data, which the Contractor believes could reasonably result in a Data Breach.

Service Level Agreement (**SLA**) means Contractor's standard service level agreement as set forth in the applicable Service Description and/or the service level agreement agreed by the parties and incorporated into a relevant Statement of Work 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 is the machine readable (object code) version of the computer programs listed from time to time on the Price List or provided with Contractor hardware and made available by Contractor for license to Customer including firmware, and any copies made, bug fixes for, updates to, or upgrades thereof. Software does not include any computer programs listed on the Price List in the name of a third party.

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 document agreed by the parties, the form of which is attached to this Agreement as Appendix A to Attachment E, that describes the particular details regarding the relevant Cloud Services offering and Purchasing Entity's service needs and expectations.

3. **Term of the Master Agreement and Purchase Orders:** The initial term of this Master Agreement is for ten (10) years with no renewal options.
   a) The term of each Purchase Order shall be stated in the Purchase Order.

   b) The term of any Purchase Order shall commence on the Effective Date of the Purchase Order and shall continue for a period of one (1) year, or such other multi-year period as set forth in the Purchase Order. Such term will be renewed automatically for successive one (1) year terms unless either party notifies the other of its intent to terminate at least sixty (60) days prior to the expiration of the then current term.
   c) Purchase Orders may not exceed the term of the Master Agreement.

4. Amendments The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

5. Assignment/Subcontracts: Neither party shall assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the other party, which will not be unreasonably withheld or delayed. Notwithstanding the foregoing, the Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint. Either party may also assign this Agreement and any right or obligation under it without the other's approval, to any affiliate. Any other attempted assignment shall be void and of no effect. Notwithstanding any assignment by the Lead State, all Participating Entities and Purchasing Entities shall remain liable for the payment of all amounts due under this Agreement.

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 for new orders of the Services provided under this Master Agreement following approved Price List updates. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination for Convenience: Unless otherwise stated, this Master Agreement may be terminated by either party for convenience upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 60 days written notice, unless otherwise limited or stated in the Participating Addendum. Any termination under this provision shall not terminate nor affect the rights and obligations of the parties regarding Orders accepted and in effect at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity

Data, rights attending default in performance an applicable Service Level Agreement in association with any Order, Contractor obligations upon termination, and any responsibilities arising out of a Data Breach. Termination of Purchase Orders for Services for convenience may only occur if expressly permitted by the applicable SOW or Service Description, and may result in termination fees as set forth in the applicable Service Description.

8. Confidentiality, Non-Disclosure, and Injunctive Relief; Intellectual Property Rights.

a) Confidentiality. Subject to the applicable law, each party (the "Receiving Party") acknowledges that it and its employees or agents may, in the course of providing or receiving Services under this Master Agreement, be exposed to or acquire information that is confidential to the other party (the "Disclosing Party"). Any reports or other documents or items (including software) that result from or are created from the use of the Confidential Information by either party 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 the Receiving Party) publicly known; (2) is furnished by Disclosing Party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in 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 Disclosing Party without the obligation of confidentiality, (5) is disclosed with the written consent of Disclosing 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) Disclosure Compelled by Law. A party will not be considered to have breached its confidentiality obligations under this Master Agreement for disclosing any Confidential Information of the other Party to the extent that such disclosure is required to satisfy any Applicable Laws, provided that the party required to make such disclosure (the "Compelled Party"):

i. promptly upon receiving any such request and within a reasonable time prior to disclosure (if possible), notifies the other party of the terms and circumstances of the requested disclosure;
ii. consults with the other party regarding the nature and scope of such request and the response or other position that the Compelled Party intends to take with respect to such request;
iii. does not obstruct or interfere with, and to the extent practical and legal, permits the other party to obtain, a protective order or other remedy to prevent, object to, enjoin, narrow the scope of, or otherwise contest the requested disclosure; and

iv. if the other party is unable to obtain a protective order or other similar remedy within a time period that is appropriate in the circumstances, then the Compelled Party will only disclose such of the Confidential Information that it is legally obligated to disclose and otherwise continue to treat such disclosed Confidential Information in accordance with this Master Agreement.

Notwithstanding termination of this Master Agreement or any Participating Addendum as described herein, the obligations of the Receiving Party with respect to Confidential Information received prior to termination shall continue for three (3) years from the date the Confidential Information was received.

c) Non-Disclosure. Each Receiving Party shall hold Confidential Information of the Disclosing Party, whether the Lead State, a Purchasing Entity, or an applicable Participating Entity, 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. The Receiving Party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. The Receiving Party shall use commercially reasonable efforts to identify and prevent any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Receiving Party shall advise Disclosing Party immediately if 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 Receiving Party shall at its expense cooperate with Disclosing Party in seeking injunctive or other equitable relief in the name of Disclosing Party against any such person. Except as directed by Disclosing Party, 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 Disclosing Party's request, Receiving Party shall turn over to Disclosing Party all documents, papers, and other matter in Receiving Party's possession that embody Confidential Information. Notwithstanding the foregoing, Receiving Party may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

d) Intellectual Property Ownership and Licenses. All Intellectual Property Rights and Confidential Information belonging to a Party (for purposes of this Section 9, Party shall include Fulfilment Partner) or its subcontractors or affiliates (i) prior to the Effective Date, (ii) during the Term, which are developed independently of the Contract, and (iii) any improvements, derivatives, or enhancements to (i) and (ii); (i)-(iii) shall collectively be referred to herein as "Background IP") will remain vested in that Party, and the other Party shall have no rights other than as expressly granted by this Agreement. In addition, Customer agrees that aspects of the Software and associated Documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Contractor. Each Party assigns its rights in the other Party's Background IP to the extent that ownership is not automatically granted consistent with this Section. Other than the above, nothing in the Contract, any Statement of Work or any Purchase Order will be deemed to alter or affect the Intellectual Property Rights of a party and/or licenses provided with any Contractor products, nor assign or transfer any Intellectual Property Rights between the Parties.

In addition, with regard to the Cloud Services:

i. Contractor's End User License Agreement (set forth on Exhibit 1 of Attachment E and incorporated into and made a part of this Agreement) shall apply, to the extent applicable to the relevant Cloud Services ordered by Customer. In addition, several of Contractor's software offerings have additional licensing terms or restrictions (Supplemental End User License Agreements, or SEULAs), which change from time to time, and/or are added as Contractor acquires or develops new software. The current SEULAs for the in scope offerings made under this Agreement are attached to Attachment F and incorporated into and made a part of the End User License Agreement, and this Agreement. If Customer wishes to amend the scope of the services to be provided, additional SEULAs may apply. The parties will negotiate an amendment to this Agreement in order to incorporate such new SEULA terms.
ii. If Purchasing Entity is required to use any third party software in the course of receiving the Cloud Services, then Purchasing Entity bears the sole obligation to

comply with the terms of any such third party software license terms.

iii. Purchasing Entity hereby grants Cloud Provider a limited, non-transferable, royalty free, worldwide license to use, copy, process and distribute the Purchasing Entity Data as reasonably required to provide the Cloud Services.

iv. The Cloud Services will not include or contemplate any joint development of any Intellectual Property Rights. To the extent either Party identifies a reason to engage in any joint development activity, the Parties will execute a separate written agreement governing such joint development.

v. All rights not expressly granted in this Agreement are reserved.

e) Injunctive Relief. Each party acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to the Disclosing Party that is inadequately compensable in damages. Accordingly, Disclosing 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. The Receiving Party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Disclosing Party and are reasonable in scope and content.

f) 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.

g) Cloud Services. In addition to the provisions above, the following additional confidentiality terms shall apply to Cloud Services:

i. Purchasing Entity acknowledges that Purchasing Entity's Confidential Information may not be logically isolated from data of Cloud Provider's other customers or suppliers. Cloud Provider agrees that (a) prior to any disclosure of or access being granted to any co-mingled third party data, unless required by law pursuant to any legal obligations to disclose third party data, the Purchasing Entity Confidential Information will be severed from and not disclosed in connection with the third party data; and (b) Cloud Provider is capable of readily locating and/or destroying Purchasing Entity's Confidential Information in accordance with this Section.

ii. Purchasing Entity will not use the Cloud Services to:

1. transmit, receive, store or process infringing, obscene, threatening, libelous, defamatory, hateful, false, misleading, fraudulent, unlawful, illegal, or tortious materials, or materials that violate another party's rights;
2. promote or distribute any viruses, Trojans, worms, root kits, spyware, adware, or any other harmful software, programs, routines, applications or technologies;
3. perform any actions that it knows or believes may disrupt the Cloud Services; or
4. attempt to gain unauthorized access to the Cloud Services, Contractor's networks or Fulfillment Partner's networks.

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.

10. 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 any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, 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;

(5) A breach of the provisions of Contractor's End User License Agreement or the provisions of this Agreement regarding Confidential Information; or

(6) Undisputed fees under a Purchase Order which are not paid when due and payment has not been received within thirty (30) days after notice from Contractor of such past due payment.

b. Upon the occurrence of an event of default, the non-defaulting party (whether Contractor, Lead State, or a Participating Entity) shall issue a written notice of default, identifying the nature of the default, and providing a period of thirty (30) calendar days in which the defaulting party 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 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 a defaulting party's liability for damages.

c. If the defaulting party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the defaulting party shall be in breach of its obligations under this Master Agreement and/or the applicable Participating Addendum, and the non defaulting party 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, or the applicable Participating Addendum or Purchase Order; and

(3) In the case of a Participating Entity, suspend Contractor from being able to respond to future bid solicitations; and

(4) In the case of a Participating Entity, suspend Contractor's performance on affected Purchase Orders; and

(5) Withhold payment or the provision of affected Services until the default is remedied.

d. Rights upon Termination or Expiration.

i. Upon termination of the Agreement, any Participating Addendum, or a Purchase Order, Purchasing Entity shall pay Contractor, as applicable, for all applicable fees due for services provided up to the date of such termination and/or termination charges (if applicable) owed under the affected Purchase Order, at the agreed-upon prices, fees, and expense reimbursement rates.

ii. Termination of a particular Cloud Service will not impact any other Cloud Service or the Contract, which will remain in full force and effect. Purchase Orders for a particular Cloud Service placed and accepted under this Agreement or any Participating Addendum prior to expiration of the contract term (even if involving a multi-year commitment) remain valid and binding in accordance with the contract terms only for the term stated therein, and shall not otherwise constitute an extension of the Master Services Agreement or such Participating Addendum.

iii. In the event of any termination pursuant to this section, and unless otherwise required by law or court of competent jurisdiction, the Lead State, Participating Entities and Purchasing Entities shall all remain obligated to comply in perpetuity with the provisions of the Contractor's End User License Agreement for the applicable Service, and provisions of this Agreement regarding Confidential Information.

e. Unless otherwise specified in the Participating Addendum or in a Purchase Order, 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 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 or applicable Purchase Order. 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, except as expressly set forth in this Agreement.

f. Exit Assistance. Upon termination of a Cloud Service and upon written request by Purchasing Entity, Cloud Provider will provide Exit Assistance in accordance with the applicable SOW. If Purchasing Entity has requested Exit Assistance, the terms and conditions of the Contract, including Purchasing Entity's obligation to pay for such Cloud Services will continue to apply to the provision of Cloud Services during the period of Exit Assistance (except no Exit Assistance fees will be owed if Participating Entity terminates the Cloud Services for breach).

11. **Changes in Contractor Representation:** The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, identified in Contractor's response to the Solicitation as responsible for the administration of this Agreement, in writing within 10 calendar days of the change.

12. **Force Majeure:** Except for the obligation to pay monies due and owing, neither party shall be in default by reason of any failure in performance of this Agreement which is outside of its reasonable control and without its fault or negligence("Force Majeure Event"). Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party on their part. The obligations and rights of the excused party shall be extended on a day-by-day basis for the time period equal to the period of the excusable delay. If a Force Majeure Event impedes Cloud Provider from providing Cloud Services, Cloud Provider will be entitled to (a) continue to invoice for the Cloud Services not affected, and (b) receive an equitable adjustment in the performance schedule that may be mutually agreed to by the Parties. When payments are delayed solely due to a Force Majeure Event, late fees with respect to such payment will not accrue during the period of such Force Majeure Event. Accordingly, Cloud Provider's delayed or defective performance or non-performance due to force majeure will not constitute a Cloud Services failure and would not be subject to any right that may be available to Purchasing Entity for an unexcused Services failure.

13. INDEMNIFICATION

a. General Indemnity. To the extent not prohibited by law, 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 of their respective successors and assigns, from and against damages, losses, liabilities or expenses, including reasonable attorneys' fees and related costs, including without limitation those based on contract or tort, arising out of or in connection with a claim, cause of action, suit, or proceeding brought by a third party for any death, injury, or damage to tangible personal property (not including lost or damaged data) to the extent caused by the negligent or intentional act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors in the course of Contractor's performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless Purchasing Entities, along with their officers, agents, and employees as well as any successors or assigns (each, an "Indemnified Party"), from and against losses, liabilities or expenses, including reasonable attorneys' fees and related costs, arising out of or in connection with claims, causes of action, suits, or proceedings, or causes of action brought by a third party claim that the Cloud Services, infringe a United States copyright existing as at the date of order or a United States patent issued as at the date of order of another person or entity ("Intellectual Property Claim"). Contractor will indemnify an Indemnified Party against any final judgment entered in respect of such an Intellectual Property Claim by a court of competent jurisdiction and against any settlements arising out of such an Intellectual Property Claim.

If an Intellectual Property Claim has been made, or in Contractor's reasonable opinion is likely to be commenced, an Indemnified Party agrees to permit Contractor, at its option and expense, either to: (a) procure for Purchasing Entity the right to continue using the Cloud Services; or (b) in the event that Contractor's actions pursuant to clause (a) are not available using commercially reasonable efforts, Contractor may terminate the Cloud Services and Contractor shall refund to Indemnified Party a pro rata portion of the price originally paid by Indemnified Party to Contractor for such Cloud Services, for the remainder of the unexpired term of the applicable Purchase Order.

(1) The Contractor's obligations under this section shall not extend to any claims arising from

a) the combination, operation or use of any Services provided by Contractor with any product, device, materials, service, equipment, devices or software not supplied by Contractor, or provided by Indemnified Party to Contractor; or

b) any modification or alteration to the Services made by any party other than Contractor, where such modification or alteration causes the infringement; or

c) revenue earned by Indemnified Party using the Services; or

d) Indemnified Party's use of any Services after:

(i) Contractor has informed Indemnified Party of modifications or changes in the Services required to avoid such Intellectual Property Claim; and

(ii) a reasonable period has elapsed to allow the modifications or changes to be instituted; and

(iii) the alleged infringement would have been avoided by implementing Contractor's recommended modifications or changes (so long as they provide equivalent functionality and performance as the Services being replaced or modified and do not require Indemnified Party to incur commercially unreasonable additional costs); or

e) Contractor's compliance with Indemnified Party's custom designs, specifications or instructions with regard to Software, equipment or materials Contractor uses in the provision of the Services, where such designs, specifications or instructions caused the infringement.

THIS SECTION STATES THE ENTIRE OBLIGATION OF CONTRACTOR AND ITS SUPPLIERS, AND THE EXCLUSIVE REMEDY OF PURCHASING ENTITY, IN RESPECT OF ANY INFRINGEMENT OR ALLEGED INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR PROPRIETARY RIGHTS. THIS INDEMNITY OBLIGATION AND REMEDY ARE GIVEN TO PURCHASING ENTITY SOLELY FOR ITS BENEFIT AND IN LIEU OF, AND CONTRACTOR DISCLAIMS, ALL WARRANTIES, CONDITIONS, AND OTHER TERMS OF NON-INFRINGEMENT WITH RESPECT TO ANY SERVICE.

Contractor's obligations to defend any claim in a. or b. above and indemnify the Indemnified Party are conditional upon the following: (a) The Indemnified Party shall promptly notify the Contractor within a reasonable time after receiving notice of such a 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 claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. (b) The Contractor shall promptly and reasonably investigate and defend any claim, but shall have full and exclusive authority 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. (c) The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for Contractor to pursue such defense and any subsequent appeal. Unless otherwise agreed in writing, this Section 13 is not subject to the limitation on direct damages set forth in Section 14.a of this Master Agreement.

14. LIMITATION OF LIABILITY and EXCLUSION OF DAMAGES

a. Limitation of Liability – Purchasing Entity. Except for those obligations under Section 13 entitled General Indemnity and Indemnity - Intellectual Property, notwithstanding anything else herein, all liability of 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) three million dollars ($3,000,000), whichever is greater. This limitation of liability is cumulative per Purchasing Entity and not per incident**.**

b. **Limitation of Liability –NASPO ValuePoint.** Except for those obligations under Section 13 entitled General Indemnity and Indemnity - Intellectual Property, notwithstanding anything else herein, all liability of Contractor, its affiliates and its suppliers to Lead State for claims arising under this Agreement or otherwise, shall be limited to the greater of $100,000, or the Administrative Fees paid by Contractor to Lead State under this Agreement in the preceding 12 month period. This limitation of liability is cumulative and not per incident**.**

c. **Waiver of Consequential and Other Damages**. In addition to the limitations set forth in both a) and b) above, in no event shall Contractor or its suppliers be liable to Lead State, a Participating Entity, or a Purchasing Entity for any incidental, special, indirect, or consequential damages, lost or damaged data, arising in tort (including negligence), or otherwise, even if Contractor or its suppliers have been informed of the possibility thereof.

15. **Independent Contractor:** The Contractor shall be 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 agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

16. **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.

17. **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 as follows:

(1) Commercial General Liability covering the risks of bodily injury (including death), property damage and personal injury, including coverage for contractual liability, with a limit of $1 million per occurrence/$2 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
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

The above limits for cloud insurance are stated as per occurrence or claim or wrongful act and in the aggregate.

The cloud insurance will be either (a) written on an occurrence form or (b) written on a claims-made form but purchased during the term of the applicable Participating Addendum and for three years after termination or expiration of such Participating Addendum.

(3) Contractor must comply with any applicable State Workers Compensation or

Employers Liability Insurance requirements.

(4) Professional Liability. Professional Liability Insurance Policy in the minimum amount of $1,000,000 per wrongful act or claim or occurrence and $1,000,000 in the aggregate, that provides coverage for its work undertaken pursuant to each Participating Addendum, and is either (a) written on an occurrence form or (b) written on a claims-made form, but purchased during the term of the applicable Participating Addendum and for three years after termination or expiration of such Participating Addendum. This professional liability insurance can be included in one and the same policy that satisfies the cloud insurance requirement.

c. Contractor shall pay premiums on all insurance policies. In the event that any of the insurance required herein is cancelled or non-renewed, Contractor shall replace such insurance so that no lapse in coverage occurs and shall provide the Lead State with a revised certificate of insurance evidencing same.

d. The Commercial General Liability insurance required herein shall (1) include the Participating Entities as additional insureds for cover liabilities falling within the indemnity obligations of the Contractor and that are otherwise covered by such insurance, and (2) provide that the Contractor’s Commercial General 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, 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, and limits of liability). 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.

18. Laws and Regulations; Modification or Discontinuation in Services: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

(a) Compliance with Law. Each party will comply with Applicable Law. Any Purchasing Entity requested changes to the Cloud Services that would result in Cloud Provider being required to secure specific additional licensing from a governmental authority that Cloud Provider does not hold as of the Effective Date of this agreement will be addressed via the Change Request Procedure set forth in Appendix B to Exhibit 2 to the Sample Cloud Services Statement of Work (the “Change Request Procedure”). Nothing in this Agreement or the Cloud Services will require either party to breach any Applicable Laws, including, without limitation, data protection or privacy laws, or require Contractor to provide Cloud Services that would result in Contractor being deemed a common carrier, legal advisor, accountant, or telecommunications provider.

(b) Cooperation. Each party will, to the extent reasonably requested by the other party and permitted by Applicable Laws, provide reasonable assistance and support to, and communicate and cooperate with, any other supplier that provides services to the other party in connection with the provision of Cloud Services. Such cooperation includes, but is not limited to following generally accepted industry practices to cooperate with one another when working with the other party's suppliers in a multi-vendor environment. If there is a material cost for such cooperation, Purchasing Entity will pay the costs for such cooperation at rates to be mutually agreed in the Change Request Procedure.

(c) Change in Applicable Law. If a change of Applicable Laws after the Effective Date requires a change in the scope of Cloud Services, at Purchasing Entity's option, Cloud Provider will be entitled to either terminate the Cloud Services or recover any reasonable additional costs it may incur by virtue of the need to change the Cloud Services to comply with any changes to such laws, and in such case the Change Request Procedure will apply. Notwithstanding the foregoing, to the extent the change of the Applicable Law affects Contractor, the cost of the modifications required as a result of such change shall be borne by Contractor. After the Effective Date and during the Term, if there are any changes to any Applicable Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto) that would restrict Cloud Provider from performing the Cloud Services ("Restrictions"), the Parties will meet to discuss and agree, in good faith, how to address the Restrictions. This may include revision of the scope of Cloud Services to implement a mutually agreeable workaround or the elimination of affected Cloud Services from the scope to address the Restrictions.

(d) Modifications and/or Discontinuance. Notwithstanding anything contained in the Master Agreement to the contrary, modifications which Contractor deems necessary to comply with specifications, changed safety standards or governmental regulations, to make the Services non-infringing with respect to any patent, copyright, or other proprietary interest, or to otherwise improve the Services may be made at any time by Contractor without prior notice to or consent of Purchasing Entity or NASPO, unless Services are materially altered, and such altered Service shall be deemed fully conforming. Contractor shall employ commercially reasonable efforts to announce, including by electronic posting, Service discontinuance or changes to the Services other than those set forth in the previous sentence in accordance with Contractor's End-of-Life Policy, which is found at the following URL: http://www.cisco.com/c/en/us/products/eos-eol-policy.html. Customer may make a last-time purchase of such Services as set forth in such policy.

19. 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 a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense 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 State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. 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.

20. Ordering and Pricing:

a. Purchasing Entity may place Purchase Orders for the various Services offered by Contractor. The provision of any such Services, if accepted by Contractor, shall be subject to the terms and conditions set forth in this Agreement, including those attached hereto as Attachment E, as well as the then-current Service Descriptions for such Service offerings.

b. Master Agreement purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

c. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms 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 Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

d. 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 the Services contemplated by this Master Agreement.

e. Contractor shall not begin providing Services without a valid Purchase Order compliant with the law of the Purchasing Entity. In addition, the Purchasing Entity and the Fulfillment Partner will also enter into Statements of Work for the applicable Contractor Cloud Services, pursuant to such Purchase Orders.

f. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

g. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The Services being delivered;
(2) The location(s) and requested start date for commencement of the Services;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The pricing consistent with this Master Agreement;
(6) A ceiling amount of the order for Services being ordered;
(7) The Master Agreement identifier and the Participating State contract identifier;
(8) Tax exempt certifications, if applicable; and
(9) any other special instructions,

h. 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.

i. Orders must be placed pursuant to this Master Agreement prior to the 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.

j. Notwithstanding the expiration or termination of this Master Agreement or the applicable

Participating Addendum, Contractor agrees to perform in accordance with the terms of any Orders then outstanding atthe time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement or the applicable Participating Addendum. Orders from anyseparate 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 or the applicable Participating Addendum, notwithstanding the term of any such indefinite delivery order agreement.

k.Changes to Cloud Services will be dealt with through the Change Request Procedure.

l. Contractor reserves the right to subcontract Services to a third party organization including Fulfillment Partners or affiliates to provide Services to Purchasing Entity, or to require that purchases be made through Fulfillment Partners or affiliates; provided that acceptance of Purchase Orders, invoicing and/or receipt of payments will only be handled by and through Contractor or its authorized Fulfillment Partners. In addition, any such subcontract shall not relieve Contractor of any of its obligations under this Agreement.

m. Any contingencies on Purchasing Entity's Purchase Orders are not binding upon Contractor. The terms and conditions of this Master Agreement and applicable Participating Addendum prevail, regardless of any additional or conflicting terms on the Purchase Order, or other correspondence from Purchasing Entity to Contractor and any additional or conflicting terms are deemed rejected by Contractor unless Contractor has expressly agreed to such terms in writing. Mere acceptance or processing of a Purchase Order containing such terms shall not constitute such express consent.

n. All Purchase Orders are subject to Contractor's reasonable acceptance (including performing any related credit checks). Contractor shall use commercially reasonable efforts to accept or reject orders in writing within ten (10) days from receipt, or within three (3) business days, if orders are placed electronically.

o. Prices for Services shall be those specified in Contractor's then current Global Price List, less any applicable Price List category or individual Service based discount(s) authorized in writing by Contractor to Purchasing Entity and valid at the time of acceptance of the Purchase Order by Contractor (a "Discount Authorization"), or in accordance with an applicable, valid written price quotation, if any, submitted by Contractor to Purchasing Entity for such Services.

p. Subject to the guaranteed minimum discount(s) provided by Contractor under the Master Agreement, Fulfillment Partners may also provide, at their sole discretion, additional, incremental discounts on a case-by-case, transactional basis.

q. All stated prices are exclusive of any taxes, fees, and duties or other similar amounts, however designated, and including without limitation value added, sales and withholding taxes, which are levied or based upon such prices, charges, or upon this Master Agreement. Purchasing Entity will pay sales and use taxes, if any, imposed on the Services acquired under this Master Agreement, or furnish proof of its tax-exempt status upon request. Contractor will pay all other taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. In the event that the Purchasing Entity is exempt from property and sales taxes, it will not be charged same.

21. 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, Order requirements, 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 c below 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 Cloud Services procured through the NASPO ValuePoint cooperative Master Agreements 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.

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. Coordination of requests for such participation shall be made 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; a Participating Entity must first ensure that it has 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 sales of goods to the general public as surplus property as required by 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.

22. Payment: Unless otherwise stipulated in the Participating Addendum, payment is due net 30 days following the date of the invoice. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of an invoice if disputed in good faith, upon written notice to Contractor. If, at any time, Purchasing Entity is delinquent in payment, or is otherwise in breach of this Agreement, Contractor may, without prejudice to other rights, withhold Services and/or require Purchasing Entity to prepay for further Services. Any sum not paid by Purchasing Entity when due shall bear interest until paid at a rate of 1 percent per month (12 percent per annum) or the maximum legal rate, whichever is less. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

23. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, affiliates, contractors and subcontractors ("Contractor Staff") who need to access the Purchasing Entity Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Purchasing Entity Data, except in the course of Cloud Data Center operations, response to service or technical issues, as required to perform the Services under 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 except those who provide the Cloud Services under this Agreement, 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 been instructed in 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.

24. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Services in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than that specified in the Solicitation, as incorporated into this Master Agreement.

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

26. Purchasing Entity Data:

No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason, except for an affiliate of Contractor or Contractor Staff, to the extent required to perform the services, unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

27. 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 administration of payments and fees ("Audit Purpose"). 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, at such party's own expense, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to payments to be made under this Master Agreement or orders placed by a Purchasing Entity under it for the Audit Purpose. This right shall survive for a period of six (6) years following termination of this Agreement or the applicable Participating Addendum, or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is latest, to assure compliance with the terms of this Agreement regarding payments.

Such access will be 1) with at least ten (10) business days advance written notice, (2) conducted during normal business hours, 3) shall not unduly interrupt or interfere with Contractor's normal business operations, and 4) in the event that such audit is conducted by a third party, such third party shall, prior to conducting such audit, execute a confidentiality agreement for the benefit of Contractor in a form reasonably satisfactory to Contractor.

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 which are documented as a result of such audit as inconsistent with the terms of the Master Agreement or orders, or Contractor will bill the applicable Lead State, Participating Entity, or Purchasing Entity for any 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 any express language in the Master Agreement that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit for the Audit Purpose relative to the applicable Participating Addendum. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense, subject to the limitations set forth in subsection (a) above.

e. From time-to-time Contractor may perform a review of Customer's use of the Services and other records (upon reasonable advance notice) to validate Service entitlement. Contractor will charge a Service fee if it finds that Services are being provided beyond that for which Purchasing Entity has paid Contractor. This Service fee includes amounts which should have been paid, interest, attorneys' fees, if any, and audit fees. Attorneys' and audit fees will only be payable by the Purchasing Entity where the discrepancy exceeds 5 percent of the amount otherwise due and payable. Contractor requires that Purchasing Entity take all necessary action (for example, disabling passwords) to ensure that any former employees or contractors do not access or use the Services.

28. 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 calculated by multiplying 0.25% against the "Net Purchase Price" paid by the Purchasing Entity. The "Net Purchase Price" is defined as Contractor's list price for all deliverables authorized for sale under this Agreement (whether they be products or services or any other deliverables), minus all applicable contract discounts, rebates or value added incentives, and excluding sales, use, or other applicable taxes, surcharges, or like fees, to the extent applicable to a Purchase Order.

For Cloud Services, Contractor will pay the administrative fee during the quarter the Purchase Order (or Change Request) was accepted by the Fulfillment Partner or in accordance with the agreed upon delivery schedule in a Purchase Order or subscription pricing arrangement. For example, for a three year Cloud Services subscription paid one year in advance, the administrative fee for the portion allocated to the first year of the subscription will be due in the quarter the initial sale is reported, while the administrative fee allocated to the second and third years will be due in the quarters that the subsequent transactions are reported, respectively.

29. **System Failure or Damage:** To the extent that system failure or damage is caused by Contractor or its Services, the Contractor agrees to use commercially reasonable efforts to restore or assist in restoring the system to operational capacity.

30. **Data Privacy:** The Contractor must comply with all Applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into an 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 in a workmanlike manner, in accordance with industry standards expected of a company providing similar Services in a similar industry, and materially as described in this Master Agreement, or any applicable Order, SLA, or Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State, to the extent Contractor's responses are incorporated into the Solicitation.

c. Contractor represents and warrants to the best of its knowledge, the accuracy of 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 will operate materially in accordance with the accompanying documentation of Service Description for such Services.

f. Except as specified in this section or in Section 9 of Exhibit 2 (EULA), Contractor hereby disclaims and Purchasing Entity waives all representations, conditions, and warranties (whether express, implied, or statutory), including without limitation, any warranty or condition (a) of merchantability, fitness for a particular purpose, non-infringement, title, satisfactory quality, accuracy, or (b) arising from any course of dealing, course of performance, or usage in the industry.

g. To the extent an implied warranty cannot be disclaimed, such warranty is limited in duration to the applicable express warranty period. Purchasing Entity's sole and exclusive remedy for breach of warranty shall be, at Contractor's option, re-performance of the Services; or termination of the applicable Purchase Order and return of the portion of the fees prepaid to Contractor by Purchasing Entity for such non-conforming Services which Purchasing Entity cannot use.

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 or the applicable Participating Addendum. 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 Contractor and the Purchasing Entity, with cost to be agreed in writing in the applicable SOW with 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, agree in writing upon 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 reasonably required by the Purchasing Entity.

33. Waiver of Breach Failure of the Contractor, 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 Contractor, Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Contractor, 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.

34. 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 to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

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.

36. **Performance and Payment Time Frames that Exceed Contract Duration:** All maintenance or other agreements for Services entered into during the duration of an Order and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and Services established per each written agreement). No new leases, maintenance or other agreements for Services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

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 Solicitation, 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 under 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. Notwithstanding any of the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights.

e. 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.

38. **No Guarantee of Service Volumes:** The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor

acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint Purchasing Entities to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provide customers information regarding the Contractor's website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the Purchasing Entity to have.

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 of the Services. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the 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 for the Cloud Services provided under this Agreement, 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 60 days following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor Cloud Services and CMSP Services will each have a separate tab in the reporting template. The reporting template will indicate the payment terms (i.e., whether the transaction was an annual subscription service paid in advance, and if applicable, how many years of pre-payment Contractor received). To the extent a transaction involves an amendment to an Purchase Order (i.e., increased capacity, renewals, or changed scope of Cloud Services), Contractor will report the amount set forth in the Change Request executed under the Purchase Order or a new Purchase Order accepted by the Partner for the renewal or additional Cloud Services, during the quarter when the Change Request is executed or new Purchase Order is received. 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; and (7) 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 sixty (60) 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. 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 60 days after the conclusion of each calendar quarter.

d. 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.

e. 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, EULA, SEULA, service descriptions, exhibits and/or other documents expressly incorporated into this agreement by reference, contains the entire understanding of the parties hereto with respect to the subject matter of this Agreement and replaces any prior oral or written communications between the parties, all of which are excluded, unless a written amendment to this Agreement is executed by the parties, or the parties to a Participating Addendum agree in writing to modify a term n a Participating Addendum. There are no conditions, understandings, agreements, representations or warranties, expressed or implied, that are not specified herein. 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, except for those EULA and SEULA terms which are attached to and incorporated and made part of this Agreement, and/or which are later agreed by the parties in a mutually executed amendment to this Agreement.

44. Severability. In the event that part of or one or more terms of this Agreement becomes or is declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such part or term shall be null and void and shall be deemed deleted from this Agreement. All remaining terms of this Agreement shall remain in full force and effect. Notwithstanding the foregoing, if this paragraph is invoked and, as a result, the value of this Agreement is materially impaired for either party, as determined by such party in its sole discretion, then the affected party may terminate this Agreement or the applicable Participating Addendum by written notice with immediate effect to the other.

45. Survival. The following sections shall survive the expiration or earlier termination of this Agreement Sections 2 (Definitions), 7 (Term and Termination), 8 (Confidentiality), 10 (Default and Remedies),12 (Force Majeure), 14 (Limitation of Liability and Consequential Damages Waiver), 22 (Payment), 31 (Warranty), 32 (Transition Assistance), 33 (No Waiver), 37 (Governing Law and Venue), 43 (Entire Agreement), 44 (Severability), 45 (Survival), 46 (Notices), Exhibit 2 (EULA) and the Glossary of Terms shall survive the termination or expiration of this Agreement.

46. Notices. Notwithstanding anything contained in the Agreement to the contrary, all notices required or permitted under this Agreement will be in writing and will be deemed given: (a) when delivered personally; (b) when sent by confirmed facsimile or electronic mail; (c) three (3) days after having been sent by registered or certified mail, return receipt requested, postage prepaid (or six (6) days for international mail); or (d) one (1) day after deposit with a commercial express courier specifying next day delivery (or two (2) days for international courier packages specifying 2-day delivery), with written verification of receipt. All communications will be sent to the addresses set forth in this Agreement or such other address as may be designated by a party by giving written notice to the other party pursuant to this paragraph. Notwithstanding the above, notices regarding general changes in pricing, policies, or programs may also be made by posting on cisco.com or by email or fax.

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

1. Purchasing Entity Data: 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 Data at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity Data and align 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 Purchasing Entity Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice for cloud providers of a similar kind, and not less stringent than the measures the Contractor applies to its own personal data and non-public Data of similar kind.

b. All Purchasing Entity Data, if required by the applicable SLA, shall be encrypted at rest and in transit with controlled access. The Encryption at rest requirement may be deleted from the SLA based on the required functionality of the service offering. Any stipulation of responsibilities to encrypt the Purchasing Entity Data will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), the applicable Participating Addendum, or otherwise made a part of the Master Agreement.

c. Unless otherwise stipulated, if required by the applicable SLA or Participating Addendum, 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 general level of protection and encryption for all Non-Public Data shall be identified in the SLA.

d. At no time shall any data or processes — that either belong to or are intended for the exclusive 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.

e. 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: If required by the applicable SLA or Participating Addendum the Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, unless these comply with Contractor's Trusted Device Standard. Notwithstanding any of the foregoing, the Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely (outside of the U.S.) 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of any 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 Purchasing Entity Data disclosed, or shall include if this information is unknown.

a. Data Breach Response: Contractor may need to communicate with outside parties regarding a Data Breach, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, or in accordance with that defined by applicable data breach notification law. Contractor shall discuss with the Purchasing Entity on an urgent as-needed basis, Contractor's communication and mitigation processes, which shall be as mutually agreed upon, or as defined by applicable data breach notification laws.

b. Data Breach Reporting Requirements: If Contractor has actual knowledge of a Data Breach which is materially impacting to the security of the Purchasing Entity, Contractor will (1) notify the Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or procedures, within 48 hours of confirmation of such Data Breach, unless a shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

5. Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Purchasing Entity 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 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 deemed necessary in Contractor's reasonable opinion.

b. Unless otherwise stipulated, to the extent a Data Breach is a direct result of Contractor's breach of its legal or contractual obligations to prevent the release of Purchasing Entity Data as set forth in the Master Agreement, the Contractor shall bear the following costs ("Data Breach Costs") associated with (1) Contractor's investigation and resolution of the Data Breach; (2)

notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service, if required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws, if required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) taking all corrective actions as reasonably determined by Contractor based on root cause. This Section 5.b states Contractor's entire obligation and State's sole and exclusive remedy for damages and expenses related to a Data Breach.

6. Notification of Legal Requests: 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 Purchasing Entity Data. 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 from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating Addendum or an SLA, the Contractor shall implement an orderly return or destruction of Purchasing Entity Data in a CSV or another mutually agreeable format and in a timeframe agreed to by the parties, or allow the Purchasing Entity to extract Purchasing Entity's data and securely dispose of it.

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 the Agreement or a Participating Addendum, the Contractor shall not take any action to intentionally erase any 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; or

- 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, upon written request of Purchasing Entity, 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, any applicable fees for access and retrieval of digital content to the Purchasing Entity will be set forth in a SOW.

d. The Purchasing Entity shall be entitled to any post termination assistance, including data retrieval, in the applicable Statement of Work.

e. Upon termination of the Services or the Agreement in its entirety, and upon written request of Purchasing Entity, 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. If deleted, Purchasing Entity Data shall be permanently deleted and shall not be recoverable. Confirmation of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. The Contractor shall provide (at its own expense) the State, upon the State's written request, with sufficient personal information about its agents or employees, and the agents and employees of its subcontractors (if any) who will enter upon secure premises controlled, held, leased, or occupied by the State during the course of performing this contract so as to facilitate a criminal record check, upon receiving the individuals' consent and in accordance with applicable law, at State expense. "Sufficient personal information" about its agents or employees, and the agents and employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any on-site work, a list of the full names of the designated employees. Individuals consenting to the criminal record check may then provide additional information to the State, including their social security number, driver license number and the state of issuance, and their birth date. Thereafter, on their first site visit, each contractor employee expected to work on-site, and who provides their consent to the State for such procedures, shall be fingerprinted by the State, and the State is authorized to conduct a federal criminal background check based upon those fingerprints and personal information provided.

b. Contractor, in executing any duty or exercising any right under this contract, shall not knowingly cause or permit any of its agents or employees, and the agents and employees of its subcontractors (if any) who have been convicted of a felony and misdemeanors other than minor misdemeanors to enter upon any premises controlled, held, leased, or occupied by the State. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred.

9. Access to Security Logs and Reports:

If required by the applicable SLA, the Contractor shall provide reports on a schedule specified in the SLA in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity, related to the infrastructure that the Contractor controls upon which the Purchasing Entity's Data resides. If required by the SLA, the 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 annually audit in accordance with the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a mutually agreed upon third party , in accordance with the terms regarding the scope of such audits as set forth in the Master Agreement.

11. Data Center Audit: If required by the applicable SLA, the Contractor shall perform an independent audit of its Data Centers at least annually and at its own expense, and provide, to the extent available, a copy of the Service Organization Control (SOC) 2 audit report upon request.

12. Change Control and Advance Notice: The Contractor shall give commercially reasonable 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 are likely to 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 within a commercially reasonable amount of time prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall discuss with Purchasing Entity how its non-proprietary system security plans (SSP) or security processes and technical limitations can provide adequate protection and flexibility between the Purchasing Entity and the Contractor. For example, regarding 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 its entirety at its discretion without interference from the Contractor at any time during the term of any Participating Addendum. 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 Contractor's 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 contractors involved in providing services at Purchasing Entity's site under this Master Agreement.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to reasonably 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 Purchasing Entity shall, subject to applicable law, have the right to request prompt removal of 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 summary business continuity and disaster recovery plan upon request and as set forth in the applicable SLA to reasonably ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (e.g., XXX hour/days shall be provided to Contractor by the Purchasing Entity.)

20. Compliance with Accessibility Standards: The Contractor shall comply with all mandatory applicable laws and regulations.

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

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption of mobile devices storing Purchasing Entity Data is consistent with commercially available validated cryptography standards.

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, upload and download (where applicable), and use Contractor's documentation.

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

1. Purchasing Entity Data: 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 Data at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity Data and align 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 Purchasing Entity Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice for cloud providers of a similar kind, and not less stringent than the measures the Contractor applies to its own personal data and non-public Data of similar kind.

b. All Purchasing Entity Data, if required by the applicable SLA, shall be encrypted at rest and in transit with controlled access. The Encryption at rest requirement may be deleted from the SLA based on the required functionality of the service offering. Any stipulation of responsibilities to encrypt the Purchasing Entity Data will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), the applicable Participating Addendum, or otherwise made a part of the Master Agreement.

c. Unless otherwise stipulated, if required by the applicable SLA or Participating Addendum, 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 general level of protection and encryption for all Non-Public Data shall be identified in the SLA.

d. At no time shall any data or processes — that either belong to or are intended for the exclusive 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.

e. 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: If required by the applicable SLA or Participating Addendum the Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, unless these comply with Contractor's Trusted Device Standard Notwithstanding any of the foregoing, the Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely (outside of the U.S.) 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of any 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 Purchasing Entity Data disclosed, or shall include if this information is unknown.

a. Data Breach Response: Contractor may need to communicate with outside parties regarding a Data Breach, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, or in accordance with that defined by applicable data breach notification law. Contractor shall discuss with the Purchasing Entity on an urgent as-needed basis, Contractor's communication and mitigation processes, which shall be as mutually agreed upon, or as defined by applicable data breach notification laws.

b. Data Breach Reporting Requirements: If Contractor has actual knowledge of a Data Breach which is materially impacting to the security of the Purchasing Entity, Contractor will (1) notify the Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or procedures, within 48 hours of confirmation of such Data Breach, unless a shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

5. Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Purchasing Entity 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 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 deemed necessary in Contractor's reasonable opinion.

b. Unless otherwise stipulated, to the extent a Data Breach is a direct result of Contractor's breach of its legal or contractual obligations to prevent the release of Purchasing Entity Data as set forth in the Master Agreement, the Contractor shall bear the following costs ("Data Breach Costs") associated with (1) Contractor's investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service, if required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws, if required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) taking all corrective actions as reasonably determined by Contractor based on root cause. This Section 5.b states Contractor's entire obligation and State's sole and exclusive remedy for damages and expenses related to a Data Breach.

6. Notification of Legal Requests: 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 Purchasing Entity Data. 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 from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating Addendum or an SLA, the Contractor shall implement an orderly return or destruction of Purchasing Entity Data in a CSV or another mutually agreeable format and in a timeframe agreed to by the parties, or allow the Purchasing Entity to extract Purchasing Entity's data and securely dispose of it.

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 the Agreement or a Participating Addendum, 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, upon written request of Purchasing Entity, and 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, any applicable fees for access and retrieval of digital content to the Purchasing Entity will be set forth in a SOW.

d. The Purchasing Entity shall be entitled to any post termination assistance, including data retrieval, in the applicable Statement of Work.

e. Upon termination of the Services or the Agreement in its entirety, and upon written request of Purchasing Entity, 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. If deleted, Purchasing Entity Data shall be permanently deleted and shall not be recoverable. Confirmation of destruction shall be provided to the Purchasing Entity.

8. Background Checks: a.. The Contractor shall provide (at its own expense) the State, upon the State's written request, with sufficient personal information about its agents or employees, and

the agents and employees of its subcontractors (if any) who will enter upon secure premises controlled, held, leased, or occupied by the State during the course of performing this contract so as to facilitate a criminal record check, upon receiving the individuals' consent and in accordance with applicable law, at State expense. "Sufficient personal information" about its agents or employees, and the agents and employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any on-site work, a list of the full names of the designated employees. Individuals consenting to the criminal record check may then provide additional information to the State, including their social security number, driver license number and the state of issuance, and their birth date. Thereafter, on their first site visit, each contractor employee expected to work on-site, and who provides their consent to the State for such procedures, shall be fingerprinted by the State, and the State is authorized to conduct a federal criminal background check based upon those fingerprints and personal information provided.

b. Contractor, in executing any duty or exercising any right under this contract, shall not knowingly cause or permit any of its agents or employees, and the agents and employees of its subcontractors (if any) who have been convicted of a felony and misdemeanors other than minor misdemeanors to enter upon any premises controlled, held, leased, or occupied by the State. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred.

9. Access to Security Logs and Reports:

a. If required by the applicable SLA, the Contractor shall provide reports on a schedule specified in the SLA in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity, related to the infrastructure that the Contractor controls upon which the Purchasing Entity's Data resides. If required by the SLA, the 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.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure as specified in the applicable SLA. 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 annually audit in accordance with the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a mutually agreed upon third party , in accordance with the terms regarding the scope of such audits as set forth in the Master Agreement.

11. Data Center Audit: If required by the applicable SLA, the Contractor shall perform an independent audit of its Data Centers at least annually and at its own expense, and provide, to the extent available, a copy of the Service Organization Control (SOC) 2 audit report upon request.

12. Change Control and Advance Notice: The Contractor shall give commercially reasonable 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 are likely to 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 within a commercially reasonable amount of time prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall discuss with Purchasing Entity how its non-proprietary system security plans (SSP) or security processes and technical limitations can provide adequate protection and flexibility between the Purchasing Entity and the Contractor. For example, regarding 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 its entirety at its discretion without interference from the Contractor at any time during the term of any Participating Addendum. 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 Contractor's 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 contractors involved in providing services at Purchasing Entity's site under this Master Agreement.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to reasonably 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 Purchasing Entity shall, subject to applicable law, have the right to request prompt removal of 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 summary business continuity and disaster recovery plan upon request and as set forth in the applicable SLA to reasonably ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (e.g., XXX hour/days shall be provided to Contractor by the Purchasing Entity.)

20. Compliance with Accessibility Standards: The Contractor shall comply with all mandatory applicable laws and regulations.

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

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption of mobile devices storing Purchasing Entity Data is consistent with commercially available validated cryptography standards.

23. 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, upload and download (where applicable), and use Contractor's documentation.

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

1. Purchasing Entity Data: 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 Data at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity Data and align 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 Purchasing Entity Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice for cloud providers of a similar kind, and not less stringent than the measures the Contractor applies to its own personal data and non-public Data of similar kind.

b. All Purchasing Entity Data, if required by the applicable SLA, shall be encrypted at rest and in transit with controlled access. The Encryption at rest requirement may be deleted from the SLA based on the required functionality of the service offering. Any stipulation of responsibilities to encrypt the Purchasing Entity Data will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), the applicable Participating Addendum, or otherwise made a part of the Master Agreement.

c. Unless otherwise stipulated, if required by the applicable SLA or Participating Addendum, 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 general level of protection and encryption for all Non-Public Data shall be identified in the SLA.

d. At no time shall any data or processes — that either belong to or are intended for the exclusive 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.

e. 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: If required by the applicable SLA or Participating Addendum 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, unless these comply with Contractor's Trusted Device Standard Notwithstanding any of the foregoing, the Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely (outside of the U.S.) 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of any 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 Purchasing Entity Data disclosed, or shall include if this information is unknown.

a. Data Breach Response: Contractor may need to communicate with outside parties regarding a Data Breach, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, or in accordance with that defined by applicable data breach notification law. Contractor shall discuss with the Purchasing Entity on an urgent as-needed basis, Contractor's communication and mitigation processes, which shall be as mutually agreed upon, or as defined by applicable data breach notification laws.

b. Data Breach Reporting Requirements: If Contractor has actual knowledge of a Data Breach which is materially impacting to the security of the Purchasing Entity, Contractor will (1) notify the Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or procedures, within 48 hours of confirmation of such Data Breach, unless a shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

5. Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Purchasing Entity 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 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 deemed necessary in Contractor's reasonable opinion.

b. Unless otherwise stipulated, to the extent a Data Breach is a direct result of Contractor's breach of its legal or contractual obligations to prevent the release of Purchasing Entity Data as set forth in the Master Agreement, the Contractor shall bear the following costs ("Data Breach Costs") associated with (1) Contractor's investigation and resolution of the Data Breach; (2)

notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service, if required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws, if required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) taking all corrective actions as reasonably determined by Contractor based on root cause. This Section 5.b states Contractor's entire obligation and State's sole and exclusive remedy for damages and expenses related to a Data Breach.

6. Notification of Legal Requests: 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 Purchasing Entity Data. 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 from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating Addendum or an SLA, the Contractor shall implement an orderly return or destruction of Purchasing Entity Data in a CSV or another mutually agreeable format and in a timeframe agreed to by the parties, or allow the Purchasing Entity to extract Purchasing Entity's data and securely dispose of it.

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 the Agreement or a Participating Addendum, 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, upon written request of Purchasing Entity, and 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, fees for access and retrieval of digital content to the Purchasing Entity will be set forth in the applicable SOW.

d. The Purchasing Entity shall be entitled to any post termination assistance including data retrieval, in the applicable Statement of Work.

e. Upon termination of the Services or the Agreement in its entirety, and upon written request of Purchasing Entity, 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. If deleted, Purchasing Entity Data shall be permanently deleted and shall not be recoverable. Confirmation of destruction shall be provided to the Purchasing Entity.

8. Background Checks: a. The Contractor shall provide (at its own expense) the State, upon the State's written request, with sufficient personal information about its agents or employees, and the agents and employees of its subcontractors (if any) who will enter upon secure premises controlled, held, leased, or occupied by the State during the course of performing this contract so as to facilitate a criminal record check, upon receiving the individuals' consent and in accordance with applicable law, at State expense. "Sufficient personal information" about its agents or employees, and the agents and employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any on-site work, a list of the full names of the designated employees. Individuals consenting to the criminal record check may then provide additional information to the State, including their social security number, driver license number and the state of issuance, and their birth date. Thereafter, on their first site visit, each contractor employee expected to work on-site, and who provides their consent to the State for such procedures, shall be fingerprinted by the State, and the State is authorized to conduct a federal criminal background check based upon those fingerprints and personal information provided.

b. Contractor, in executing any duty or exercising any right under this contract, shall not knowingly cause or permit any of its agents or employees, and the agents and employees of its subcontractors (if any) who have been convicted of a felony and misdemeanors other than minor misdemeanors to enter upon any premises controlled, held, leased, or occupied by the State. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred.

9. Access to Security Logs and Reports: a. If required by the applicable SLA, the Contractor shall provide reports on a schedule specified in the SLA t agreed to by the parties, directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. If required by the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity Data 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 as specified in the applicable SLA. 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 annually audit in accordance with the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a mutually agreed upon third party , in accordance with the terms regarding the scope of such audits as set forth in the Master Agreement.

11. Data Center Audit: If required by the applicable SLA, the Contractor shall perform an independent audit of its Data Centers at least annually and at its own expense, and provide, to the extent available, a copy of the Service Organization Control (SOC) 2 audit report upon request. . .

12. Change Control and Advance Notice: The Contractor shall give commercially reasonable 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 are likely to 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 within a commercially reasonable amount of time prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall discuss with Purchasing Entity how its non-proprietary system security plans (SSP) or security processes and technical limitations can provide adequate protection and flexibility between the Purchasing Entity and the Contractor. For example, regarding 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 its entirety at its discretion without interference from the Contractor at any time during the term of any Participating Addendum. 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 Contractor's 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 contractors involved in providing services at Purchasing Entity's site under this Master Agreement.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to reasonably 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 Purchasing Entity shall, subject to applicable law, have the right to request prompt removal of 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 summary business continuity and disaster recovery plan upon request and as set forth in the applicable SLA to reasonably ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (e.g., XXX hour/days shall be provided to Contractor by the Purchasing Entity.)

20. Compliance with Accessibility Standards: The Contractor shall comply with all mandatory applicable laws and regulations.

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

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption of mobile devices storing Purchasing Entity Data is consistent with commercially available validated cryptography standards.

23. 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, upload and download (where applicable), and use Contractor's documentation.

.

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 % ___10%___**

Infrastructure as a Service **Discount % ___10%___**

Platform as a Services **Discount % __10%____**

Value Added Services **Discount %___0%____**

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate $ __NTE $600.00________
Remote Hourly Rate $ NTE $525.00___________

Professional Services

- **Deployment Services** **Onsite Hourly Rate $ NTE $743.17____________**
  Remote Hourly Rate $ NTE $661.17___________
- **Consulting/Advisory Services** **Onsite Hourly Rate $ NTE $743.17____________**
  Remote Hourly Rate $ NTE $661.17___________
- **Architectural Design Services** **Onsite Hourly Rate $ NTE $743.17____________**
  Remote Hourly Rate $ NTE $661.17___________
- **Statement of Work Services** **Onsite Hourly Rate $ NTE $743.17____________**
  Remote Hourly Rate $ NTE $661.17 ___________

Partner Services **Onsite Hourly Rate $ NTE $600.00____________**
Remote Hourly Rate $ NTE $525.00

Training Deployment Services **Onsite Hourly Rate $ NTE $600.00____________**
Online Hourly Rate $ NTE $525.00____________

Cisco Systems, Inc. Response to Request for Proposal

NASPO ValuePoint Cloud Solutions

SOLICITATION NO. CH16012

March 10, 2016

Cisco Systems, Inc. Response to Request for Proposal

NASPO ValuePoint Cloud Solutions

SOLICITATION NO. CH16012

March 10, 2016

Cisco Systems, Inc.

Cover Letter

March 10, 2016

Mr. Christopher Hughes
Contract Analyst
1 State Office Building - Suite 3150
Salt Lake City, Utah 84114

Subject: NASPO ValuePoint Cloud Solutions Solicitation No. CH16012

Dear Mr. Hughes

Cisco Systems, Inc. is pleased to submit its technical and cost proposal through this transmittal letter to the State of Utah and NASPO ValuePoint in response to the above-referenced Request for Proposal (RFP) for Cloud Solutions. Cisco is proud of its partnership with NASPO ValuePoint and the Participating States under our current Data Communications AR-233(14-17) contract and the previous one since 2007. This rich experience has allowed us to fully understand and appreciate the NASPO ValuePoint requirements under this RFP from both the OEM and end-user perspectives.

Cisco is offering cloud services in each of the three service models available (SaaS, IaaS, and PaaS) with various deployment models offered specific to each service varying from public to private. Please see our technical response for a full listing of Cisco offerings proposed. Cisco is offering cloud services with each offering having various levels of customer data as part of the services. Our offerings all provide the ability to store low risk customer data classifications, if applicable. Some offerings may provide the ability to store Medium or even High risk data. For example, our Webex offering has become FEDRAMP certified and may be able to meet the high risk classifications for storage and security. See our technical response for further details of the specific offerings proposed.

Cisco fully understands and greatly appreciates that we will have the opportunity negotiate the Master Agreement and Participating Addendums with the Participating States/Participating Entities. Cisco is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs. Cisco understands, agrees and fully support 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.

We strongly believe that our response meets the requirements as called out in this State of Utah/ NASPO ValuePoint Cloud Solutions Solicitation No. CH16012, except as annotated in our response. If the State of Utah or NASPO ValuePoint determines that

Cisco's response is deficient in any way, Cisco respectfully requests to be promptly notified and be given the opportunity to correct any such deficiency. Please forward any general questions regarding this solicitation response to:

Ms. Mimi Nguyen-Farr, Sr. Manager USPS Contracts Management Office
Office: (408) 527-2627
Cell: (650) 228-8748
Email: mimnguye@cisco.com

Please feel free to also contact the following key individuals who have been major contributing leads to this bid response:

Proposal Lead and BidSync Submitter:
Curtis Milligan, Proposal Manager
Office: (703) 484-0067
Cell: (843) 442-3913
Email: cmilliga@cisco.com

Cisco Cloud Subject Matter Expert
Chris Castaldy, BD/Capture Manager
Office: (703) 484-0094
Cell: (540) 878-9334
Email: chcastal@cisco.com

This proposal was prepared internally by a cross-functional team of highly experienced, senior professionals from our U.S. Public Sector organization as well subject matter experts from Cisco's Cloud Business Units:

- Business Development/Capture (Chris Castaldy)
- Cloud Business Units (Multiple Leads, SMEs and Product Marketing Managers)
- Contracts Management Office (Mimi Farr, Charlie Grove)
- Legal Counsels (Leslie DeCillis, Kerry Yun)
- Proposals/Solicitations (Curtis Milligan and Staff)
- State of Utah Sales (Bruce Larson)

On behalf of Cisco, thank you for giving us the opportunity to respond to this RFP and we look forward to continuing a mutually rewarding partnership.

Sincerely,
John Christoph
John Christoph
Director.Finance

APPROVED BY LEGAL

Acknowledgment 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.

Cisco Systems, Inc.
Offeror

John Christoph John Christoph - Director.Finance
Representative Signature

3/9/2016

APPROVED BY LEGAL

Legal Disclaimer

Thank you for the opportunity to submit this non-binding (other than pricing for now-available products listed in our quotes) proposal for your consideration. Please note that this proposal may include proprietary, confidential, and/or trade secret information which, if included, will be clearly marked as such in the proposal. Any information that Cisco considers to be a trade secret will not be subject to disclosure under any public records act.

This proposal is valid for a period of ninety (90) days from the date of proposal submission.

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Cisco is a registered trademark of Cisco Systems, Inc.

The Cisco logo is a registered trademark of Cisco Systems, Inc.

Cisco WebEx is a registered trademark of Cisco Systems, Inc.

Cisco ONE is a registered trademark of Cisco Systems, Inc.

Table of Contents

List of Figures

List of Tables

List of Attachments

Legal Company Name (include d/b/a if applicable) Cisco Systems, Inc.	Federal Tax Identification Number 77-0059951	State of Utah Sales Tax ID Number VC0000118462	
Ordering Address To be provided once authorized resellers are selected for each participating addendum. This information will be posted on the required website. Same process as today.	City	State	Zip Code
Remittance Address (if different from ordering address) To be provided once authorized resellers are selected for each participating addendum. This information will be posted on the required website. Same process as today.	City	State	Zip Code
Type Corporation □ Corporate Entity (not tax-exempt)	Company Contact Person Mimi Nguyen		
Telephone Number (include area code) 408.527.2627	Fax Number (include area code) 408.608.1802		
Companys Internet Web Address http://www.cisco.com	Email Address mimnguye@cisco.com		
Discount Terms (for bid purposes, bid discounts less than 30 days will not be considered)	Days Required for Delivery After Receipt of Order (see attached for any required minimums)		
Offeror=s Authorized Representative=s Signature John Christoph	Date 3/9/2016		
Type or Print Name John Christoph	Position or Title Director Finance		

APPROVED BY LEGAL

Executive Summary

As a global leader in IT and cloud solutions powering todays largest cloud customers in enterprise, government, and service providers, Cisco has a full line of IT products and services. With our comprehensive set of cloud solutions, you can create, build and deploy a cloud strategy that is not just public vs. private, but a multi-cloud strategy allowing the mobility of workloads securely across public and private clouds. One of the most appealing qualities of the cloud is the variety of ways that it can be delivered and consumed. A successful cloud strategy will let the State of Utah, Division of Purchasing (Lead State) and the NASPO Value Point Cooperative Purchasing Program Participating Entities take advantage of the full range of consumption models for cloud services to meet their specific organizational needs. The type of cloud solution you choose may depend on the applications you are using, TCO, security needs, and SLAs.

Cisco provides a highly flexible platform for delivering the powerful capabilities that you and your governmental organizations require. Cisco believes that the network is the foundation for cloud internetworking. The network connects users to clouds and also links various cloud services and sites together. In addition, within a cloud-based IT environment, the network is the fabric that securely links all of the cloud elements into a cohesive whole. As it performs these various functions, the network becomes the optimal place to control performance and apply security, while monitoring the overall system to maintain service levels. As a leader in networking for the Internet, Cisco is well positioned and focused on helping the State of Utah and other participating states to utilize this knowledge in developing and procuring their cloud strategy and applicable services.

Cisco offers a broad set of capabilities that help you meet the unique needs of users and organization functions. Because one size does not fit all when determining the type of cloud service and its applicable deployment model, Cisco has developed cloud solutions that encompass infrastructure as well as applications in various categories of services including:

- Collaboration
  - WebEx
  - Spark
  - Tropo
- Security
  - Cloud Email Security
  - Cloud Web Security
- Infrastructure
  - Metapod
  - Meraki
  - Energy Management
  - Cloud Consumption as a Service

Cisco Cloud Solutions—*A secure cloud platform for all NIST service models.*

The Cisco Cloud Portfolio is built on validated architectures, innovative infrastructure solutions, and best practices. Cisco can help agencies provide the best combination of Cisco powered cloud services. Cisco Services for Cloud Strategy, Management, and Operations can work closely with agency personnel to enable agencies to become a trusted broker of IT services, progress on their journey to the cloud, and get there quickly and efficiently.

The Cisco Collaboration portfolio provides integrated collaboration capabilities, including IM, presence, voice, video, conferencing, and content sharing across devices for every aspect of an organization. The Cisco Collaboration Architecture is built on an integrated and open platform that embraces mobility, video, and cloud. This architecture supports anytime, anywhere collaboration among employees, citizen customers, and partners. In addition to reducing the complexity of the IT environment, the collaboration products offer tangible benefits in the way of decreased costs, increased efficiency, and more innovation. The Cisco portfolio allows employees to choose the best collaboration option for each situation. IT can integrate Cisco products within existing environments and technology and benefit from flexible implementation options, including cloud and on-premises, for speed and agility in deployment.

Cisco Cloud — Flexible Consumption Choices

A rich variety of cloud consumption models are available in our proposal. Cisco offers a comprehensive set of market-leading technologies and services for faster IT and cloud innovation. Using our experience working with many customers worldwide, we can help agencies build and manage cloud deployments. Our solutions combine our extensive experience, knowledge, and best practices with our constantly expanding portfolio of cloud offerings (**Table 1**).

Table 1. A Diverse Array of Cisco Cloud Models Available to Meet Specific Needs

Cisco Cloud Offering	Cloud Service Model	Deployment Models	Location
Metapod	IaaS	Private, Hybrid	Customer Premises
WebEx	SaaS	Public, Community	Service Provider
Spark	SaaS	Public	Service Provider
Cloud Email Security	SaaS	Hybrid	Service Provider
Cloud Web Security	SaaS	Hybrid	Service Provider
Meraki	SaaS	Hybrid	Service Provider
Tropo	PaaS	Public	Service Provider
Cisco Energy Management	SaaS	Public	Service Provider

Cloud Consumption as a Service	SaaS	Public	Service Provider

Cisco provides a highly flexible platform for delivering the powerful capabilities that organizations require today to improve the delivery of digital services to their customer citizens. Cisco is a proven partner supporting agencies in their journey to the cloud. Customers working with Cisco to plan, build, and manage their cloud initiatives have reduced TCO by more than 50 percent, enabled more efficient resource utilization, reduced TCO of collaboration applications by 15 to 23 percent, and accelerated revenue attainment through new organization models. Our strategy provides industry leading perspective and expertise that can significantly increase cloud implementation and adoption success. As a valued Strategic Partner to the State of Utah and NASPO ValuePoint, we are pleased to provide our proposal and we look forward to continuing our strategic relationship in the future.

Mandatory Minimums

5.5 (M) 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.

Cisco Response:

Read and understood.

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.

Cisco Response:

Because Cisco's technologies are not off-the-shelf purchasable items, they have to be individually configured. Consequently, we will be pursuing the Hosted Catalog structure with SciQuest since the Punch-Out catalog model is not a viable option for us. However, we would still need to understand the exact format to execute the Hosted catalog structure for Cisco's offerings.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment[1]. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), **Exhibit 1 to Attachment B**, or to 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 documents.

Cisco Response:

Cisco has provided a completed CAIQ for each of our service offerings and we warrant the accuracy and currency of the information provided within the CAIQ. Due to the sensitivity of the information provided, Cisco has provided only the CAIQ. We believe that the CAIQ helps provide a solid foundation for assessing the risk models and controls for each of our cloud offerings. If additional information is required, Cisco would be happy to meet and discuss further.

5.5.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement[2], which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements

[1] CSA STAR Self-Assessment documents the security controls provided by an Offeror's offerings, thereby helping Purchasing Entities assess the security of an Offeror, if awarded a Master Agreement, they currently use or are considering using.

[2] SLAs can vary depending on the cloud service being procured as well as the individual ordering activity, and the Lead State does not expect to require a single SLA to all cloud solutions being proposed under the RFP. Additionally, by submitting a sample the Lead State does not agree to its terms and you understand that a Purchasing Entity may revise the SLA to conform to the requirements of its laws.

Cisco Response:

Cisco has provided a sample Service Level Agreement for each of its cloud offerings proposed, as applicable. Please see the Section 8.10.2 for information about our sample Service Level Agreements. The Service Level Agreements vary according to cloud offering and therefore, several samples are provided in Attachment 3 Service Descriptions and SLAs.

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.

Cisco Response:

If awarded a contract under this RFP, Cisco will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in this proposal.

Business Profile

6 BUSINESS INFORMATION

6.1 (M)(E) 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.**

Cisco Response:

Cisco was started in 1984 by a husband and wife team, Len Bosack and Sandy Lerner, who were involved in running Stanford University's computer operations. Cisco was incorporated in the State of California in 1984 and went public on February 16, 1990. Today, we have over 70,000 employees in over 400 offices worldwide that design, produce, sell, and deliver integrated products, services, and solutions. Cisco has one of the lowest attrition rates in the IT industry.

Cisco has one of the strongest financial foundations in the industry. Our solid financial history, which is based on outstanding revenue and earnings over time, allows us to offer industry-leading products and excellent customer satisfaction and support.

Cisco Revenue and Some Financial Indicators over Past 5 Years

In millions, except Revenue, please see **Table 2**.

Table 2. Cisco Revenue and Some Financial Indicators over Past 5 Years

	FY2015 (ended 07/25/15	FY2014 (ended 07/26/14	FY2013 (ended 07/28/13	FY2012 (ended 07/28/12	FY2011 (ended 07/30/11)
Revenue	$49.2 billion	$47.1 billion	$48.6 billion	$46.1 billion	$43.2 billion
EBITDA*	11,129	9,620	11,591	10,448	8,194
Operating Income	10,770	9,345	11,196	10,065	7,674
Net Change in Cash	151	(1,199)	(1,874)	2,137	3,081
Retained Earnings	16,045	14,093	16,215	11,354	7,284

*EBITDA is earnings before interest, taxes, depreciation, and amortization

6.2 (M)(E) 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 business provided offerings identical or very similar to those required by this RFP. Government experience is preferred.

Cisco Response:

Cisco currently holds 45 direct government contracts with State and Local governments across the U.S., including the NASPO ValuePoint Data Communications Master Agreement and associated 24 Participating Addendums with ~520 authorized resellers as our fulfillment partners under these contracting vehicles. Cisco has a dedicated Contracts Management Office led by Ms. Mimi Nguyen-Farr to implement, administer, and ensure compliance of these direct contracts and coordinate contract-related activities with Cisco Sales, Channels, and the authorized resellers. Because cloud-specific contracts are relatively new, **Table 3** lists Cisco's current largest contracts in the last 2 years that does include some of the offerings that Cisco is including in its bid response.

Table 3. Largest Contracts and Net Sales

Contract	*2014 Total Net Sales*	*2015 Total Net Sales*	*Total*
WSCA/NVP #AR233	$230,000,000	$317,500,000	$547,500,000
NY - OGS	$163,000,000	$190,000,000	$353,000,000
TX - DIR Branded	$52,000,000	$154,700,000	$206,700,000
MN - 41910	$33,000,000	$37,200,000	$70,200,000
VA- VASCUPP	$38,000,000	$37,600,000	$75,600,000
Top 5 Total Net Sales	**$516,000,000**	**$737,000,000**	**$1,253,000,000**

6.3 (M) 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.

Cisco Response:

Please refer to Cisco's Dun & Bradstreet (D&B) report for the applicable year. Per D&B policy, companies must request this report directly from D&B. Our D&B number is 15-380-4570. Dun & Bradstreet Composite Rating of 5A2. Cisco's last 2 years of financial statements can be found in:

- Attachment 1 FY2015-Income-Statements-GAAP-Reconciliation
- Attachment 2 FY2014_Income_Statements_GAAP_Reconciliation

6.4 (E) 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.

Cisco Response:

Cisco Cloud Strategy

Cisco has developed a comprehensive cloud strategy that will continue to help us capitalize on this powerful trend. We can put our strategy to work for you and help you achieve a high level of business flexibility, reduce risk, and boost your agility and competitiveness. Our ecosystem-based and partner-centric strategy is built on five major pillars (see **Figure 1**).

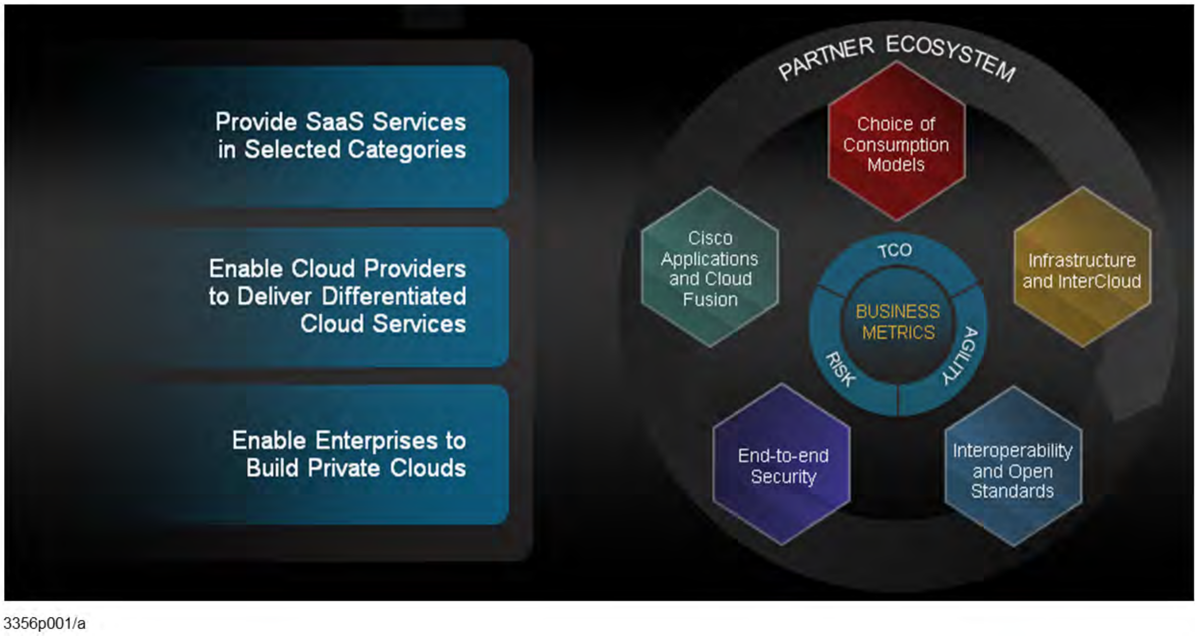

Provide SaaS Services in Selected Categories
Enable Cloud Providers to Deliver Differentiated Cloud Services
Enable Enterprises to Build Private Clouds
PARTNER ECOSYSTEM
Choice of Consumption Models
Cisco Applications and Cloud Fusion
Infrastructure and InterCloud
TCO
BUSINESS METRICS
RISK
AGILITY
End-to-end Security
Interoperability and Open Standards
3356p001/a

Figure 1. Cisco Cloud Strategy

Your Choice of Consumption Models

One of the most appealing qualities of the cloud is the variety of ways that it can be delivered and consumed. A successful cloud strategy will let you take advantage of the full range of consumption models for cloud services to meet your specific business needs. The type of cloud solution you choose may depend on the applications you are using, TCO, security needs, and SLAs.

Cisco enables businesses to build private clouds, and enables cloud providers to deliver differentiated cloud services. We also offer SaaS in selected categories in which we have unique intellectual property. In essence, together with our partners, we give you complete freedom of choice. You may even want to employ a mix of public and private clouds, to take advantage of a hybrid cloud environment that is tailored to your business needs.

If you are seeking to build a private cloud environment, Cisco offers a comprehensive portfolio of integrated infrastructure solutions, cloud management, and automation software. We also provide professional services to help you plan, build, and manage your cloud environment and keep it running at its best.

Our partners offer a variety of Cisco Powered Cloud Services. As the industry standard for cloud and managed services, Cisco Powered offerings help you achieve faster time to value and experience assured performance that scales to meet your changing business needs. Our solutions help you lower your operating costs and reduce risk by reducing complexity during the entire technology lifecycle. These capabilities free your organization to focus on its core competencies. Because providers must undergo rigorous certification and a third-party audit of their solutions, each Cisco Powered Cloud Service has been verified to deliver superior service, security, and support 24 hours a day, 7 days a week. You'll also stay ahead of your competition by taking advantage of industry-wide innovation from Cisco's extensive R&D investment and leadership in advancing open standards. You can choose from a variety of services. Your cloud provider will work closely with you to understand your business and develop a solution that is tailored to your needs.

You can also purchase complete Cisco cloud services directly from Cisco to support specific applications and services. Cisco offers cloud solutions that build on our expertise in collaboration, security, network management, and many other areas.

Infrastructure and Intercloud

Your business is constantly evolving and changing, so your technology will need to be flexible to handle change as well. To be built to last, a cloud solution should be based on a modular, scalable, and programmable infrastructure. A fabric-based, common platform for physical, virtual, and cloud services, together with a common operating model, gives you a solid foundation with room to grow. Programmability enables Development and Operations (DevOps) processes and application agility. Our customers and cloud providers both expect an open, programmable solution to master the art of provisioning, automating, and managing their servers. This combined model facilitates automation, makes IT management easier and more efficient, and helps your organization be more productive and agile.

Our integrated infrastructure solutions bring together the industry's most powerful data center technologies to make rolling out the applications you need fast and simple. To avoid getting locked into one specific deployment model or public-cloud service provider, you also need support for open and secure migration of IT services across hybrid cloud environments. This implies the capability for you to be in control: for you to deploy your applications and data in a public cloud and have them return to your data center secure and intact according to your policies and business needs. Open and secure inter-cloud portability of applications should be an option for you to use.

Cloud technology is constantly moving forward, guided by innovations such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and network programmability. The network is critical to the cloud. Every cloud is some combination of a service and deployment model. Regardless of the type of cloud, however, one fact remains true: no network means no cloud. Without networks, users cannot access their cloud services. Without networks, applications, data, and users cannot move between clouds. Without networks, the infrastructure components that must work together to create a cloud cannot do so. Our multi-cloud model is designed to evolve to adopt the latest developments in cloud computing. Our solutions use consistent, open APIs to support a common framework and programmability model across enterprises and cloud providers for hybrid cloud deployments and consistency across cloud providers.

Cisco Applications and Cisco Cloud Fusion

The promising potential of the cloud, together with evolving user demands, is changing the way that IT views the deployment of applications. Businesses want the capability to use the best of on-premises solutions and the best of the cloud. Cisco Cloud Fusion lets you use the best solutions and extend them to all. Connect and collaborate your way — across multiple applications and platforms, using any consumption or deployment model, with confidence and without compromise. Cisco Cloud Fusion brings together clouds and fuses applications that are cloud based with on-premises applications. The result is a complete set of secure, manageable applications, delivered in the way that makes sense for your business. Cisco Cloud Fusion puts the power of the World of Many Clouds to work for you.

Our cloud-based Cisco Web Security and network management offerings provide additional SaaS capabilities to help you control risk and simplify network administration. And if you want to support a specific enterprise software application such as SAP, you can work with a number of Cisco partners who can build and deliver a tailored SaaS solution.

Interoperability and Open Standards for Cloud

Your cloud environment does not run in a vacuum. It needs to interact smoothly across a wide world of network components, applications, and services that make up today's extended enterprise. There is no reason to be locked into a particular vendor's solution. That is why Cisco is committed to an open, interoperable, and standards-based approach to the cloud. Our strategy is to support multiple cloud approaches, give you choice and flexibility, and serve our customers' business needs.

OpenStack is an important part of our strategy for companies that want to purchase or deliver cloud solutions. It is an international open source cloud operating system developed by a community of developers and organizations. OpenStack is designed to make it easier to provision and scale out IT resources and applications. Our open source, standards-based infrastructure is designed to work smoothly with other OpenStack development environments and investments from our partners and customers.

Cisco also is a member of leading industry organizations that promote cloud standards, such as the Cloud Standards Customer Council and the Cloud Security Alliance.

End-to-End Security

In an environment of changing threats and new regulations, security, compliance, and data sovereignty laws are main considerations for every organization, regardless of the size or industry. No matter what type of solution you are employing, you and your cloud provider share responsibility for compliance with government and industry regulations such as HIPAA, the Federal Information Security Management Act (FISMA), Payment Card Industry (PCI) requirements, and other mandates.

To safeguard your sensitive business data and protect your customers and your reputation, you need complete end-to-end security that spans your network and your cloud services environments. In the past, traditional security solutions such as firewalls could protect your network perimeter and provide strong security. But hybrid cloud environments need protection that extends across your physical, virtual, and cloud domains. Your security policies need to be agile and consistent, too. They must adapt to constantly changing traffic patterns that derive from the cloud's dynamic consumption models.

A Comprehensive Ecosystem

Employing a strategic approach to the cloud is crucial to planning a successful cloud deployment. But to make this vision a reality, you need to partner with a vendor that can deliver the products, complete solutions, and services — all backed by expert partners who understand your business.

Cisco uses an ecosystem approach to delivery of cloud solutions. Together with our partners, we align our cloud portfolio with our strategy to provide a complete cloud solution that is tailored to your needs and helps you control costs, build a more agile business, and better manage risk.

Cloud is transforming today's businesses, enabling them to become more agile, flexible, and productive — while controlling costs and reducing risks. By employing a carefully planned cloud strategy, you can empower your IT department to be more proactive and help guide critical business priorities. A partnership with Cisco is an excellent way to get started moving forward to embrace today's World of Many Clouds.

Cisco Cloud Portfolio

The Cisco Cloud Portfolio, in conjunction with our partner ecosystem, offers NASPO ValuePoint participating entities a way to move beyond its traditional focus on operations and management to support strategic business objectives and better serve its stakeholders. The Cisco Cloud Portfolio offers the best cloud offerings to achieve a wide range of business goals while also retaining control, lowering costs, increasing business agility, and reducing risk. This in turn enables IT and business to buy and consume IT together; in harmony and against a strategic plan in which business objectives are fused with IT strategy.

Overview

Cisco's cloud portfolio transparently integrates the three pillars of cloud computing – Cisco Cloud Intelligent Network, Cisco Unified Data Center, and Cisco Cloud Applications – to deliver security while redefining scalability, flexibility, and QoS for any device in any location. Cisco provides the platform on which innovation is built: the kind of innovation that allows businesses to truly achieve the promise of the World of Many Clouds.

Build Your Cloud

Cisco enables you to build and retain complete control of a private cloud environment and, in fact, Forrester has rated us number one for private cloud strategy.[3] In addition, you can use Cisco for multiple cloud deployment models, and provide a solid foundation for your cloud-based services—private, public, or hybrid. Rated by Synergy Research Group as the leader of the cloud infrastructure equipment market the past 3 quarters, our integrated infrastructure solutions provide the validated, fabric-based common platforms you need. They are based on industry and open source standards, such as OpenStack, to accelerate deployment and deliver the right quality of service. Community innovation is creating new opportunities for cloud computing. Many organizations are turning to OpenStack software to create massively scalable cloud infrastructures. Cisco's unified data center infrastructure provides the underlying foundation for OpenStack, helping IT departments transform their complex environments into agile and secure cloud infrastructures that costs less to operate and maintain.

At any stage of your cloud journey, consider a Cisco Domain Ten engagement.[4] This industry-unique framework, embraced by global businesses to guide their IT and data center transformation, helps you methodically plan the next stages of your organization's journey to the cloud. Starting from your current state of readiness, you gain a holistic view of your IT environment, and then project your desired state and identify the gaps that must be filled to address infrastructure, application, security, compliance, process, and governance implications for your cloud plans.

Expert consultants then support your build phase with Cisco Cloud Enablement Services for Building Clouds, which provide customized strategy, planning and design, implementation, and optimization services. And Cisco Cloud Enablement Services for Adopting Clouds accelerate the adoption of public and hybrid clouds, based on your current environment and business goals. Build security into your solution to reduce your exposure to breaches with Cisco Cloud Security Services, which span the entire cloud lifecycle. In the recent IDC MarketScape Cloud Professional Services survey,[5] Cisco was named a Worldwide Major Player for cloud professional services. We have people, processes, and tools resulting from more than 28 years of industry experience, more than 50 million devices, and more than 6 million customer encounters every year that you can use to your advantage.

Manage Your Cloud

Forrester[6] ranked Cisco in the top three for cloud management (Cisco IAC) and infrastructure management (Cisco UCS Director). Cisco IAC is a comprehensive cloud management platform

[3] The Forrester Wave: Private Cloud Solutions, Q4 2013: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6505/ps11869/the_forrester_wave__private_cloud_solutions__q4_2013.pdf

[4] Cisco Domain Ten: http://www.cisco.com/web/offers/domain_ten.html

[5] IDC MarketScape: Worldwide Cloud Professional Services 2013 Vendor Analysis, Doc #242401, August 2013: http://idcdocserv.com/242401e_Cisco

[6] The Forrester Wave: Private Cloud Solutions, Q4 2013: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6505/ps11869/the_forrester_wave__private_cloud_solutions__q4_2013.pdf

that delivers a solid foundational private and hybrid cloud platform that easily expands to more sophisticated use cases such as PaaS, network automation, and anything as a service. Cisco IAC meets your private and hybrid cloud solutions cloud service delivery demands with room to grow cloud service delivery across your entire organization.

The Cisco Intelligent Automation for Cloud Design and Deployment Service assists you in building your standard or custom interface portal. Cisco UCS Director delivers unified infrastructure management for administering computing, network, virtualization, and storage from one self-service web interface, with Cisco Data Center Design and Deployment Service for Cisco Intelligent Automation for Cloud supporting implementation.

Managing and provisioning cloud resources is made easier with OpenStack,[7] an open source cloud operating system. Cisco Services for OpenStack helps you evaluate requirements and implications and supports deployment on Cisco UCS cloud architecture. The result is an open source platform giving you a tremendous choice of cloud solutions from an ecosystem of industry-leading technologies.

Extend Your Cloud

When you are ready to extend and integrate your hybrid cloud, Cisco has a solution for that as well. With Cisco InterCloud, you can create an open, transparent, and secure hybrid cloud environment across multiple cloud providers and between your premises-based applications and the public cloud. Retain complete control and security with a hybrid cloud orchestration and management framework, and help ensure consistency of network and security policies. Under the Cisco ONE umbrella, Cisco InterCloud can be integrated into higher-level management solutions, such as Cisco IAC or other cloud management solutions that our ecosystem partners provide.

Discover the extent of the hidden cloud (“shadow IT”) within your organization with Cisco Cloud Consumption Services that harness network intelligence to analyze your cloud use, risk profile, and cloud spending, enabling informed decisions to better manage risks and costs. Next, engage Cisco Business Readiness Services to help articulate the strategy and develop the business case, and an architecture-led master plan for your cloud transformation and move to hybrid cloud.

Accelerate Your Cloud ROI

Start reaping the benefits of your cloud initiative faster. Cisco Services for Cloud Strategy, Management, and Operations, available from expert Cisco consultants and our channel partners, guide you in assessing opportunities and developing and implementing your unique cloud strategy and plan.

Use our plan-build-manage IT lifecycle services to achieve three critical success factors for your cloud strategy: the optimal mix of cloud consumption models, reduced exposure to business and IT risks during your transition and cloud service delivery, and the capability to intelligently automate the cloud environment. This fuels a competitive advantage, including new business

[7] OpenStack: http://www.cisco.com/web/solutions/openstack/index.html

models, new market opportunities, and the capability to monetize business assets, all while reducing your total cost of ownership.

Cisco Services for Cloud On-Boarding Acceleration help you more quickly migrate applications to your cloud and realize the value of your infrastructure, automation, and operations investment.

To support newly deployed cloud solutions, customers can now use Cisco Data Center Solution Support Service for Critical Infrastructure to contact Cisco directly and receive overarching, coordinated multivendor data center expertise, supplementing product support offers from Cisco and our technology partners.

Cloud-Based Collaboration Solutions

Businesses want the capability to enjoy the best of on-premises solutions and the best of the cloud. Cisco Cloud Fusion enables customers to use the best solutions and extend them to all. Connect and collaborate your way—across multiple applications and platforms, through any consumption or deployment model, with confidence and without compromise. Cisco Cloud Fusion brings together clouds and fuses applications that are cloud based with those on premises, making them manageable and secure.

Cisco Powered cloud services[8] are available from certified Cisco partners, offering the entire Cisco Collaboration portfolio—including voice, video, and telepresence, messaging, IM, presence, web conferencing, customer collaboration and contact center, and mobility solutions.

Also available from the public cloud are Cisco WebEx services, providing industry-leading web conferencing capabilities. Cisco WebEx is interoperable with Cisco Unified Communications products, delivering a superior cross-platform experience.

Additional Cisco Cloud-Based Applications

In addition to cloud-based collaboration, you can purchase cloud-based web security and network management services directly from Cisco. Cisco Meraki simplifies management of wired and wireless networks. Cisco Cloud Web Security protects and provides policies for securing your web deployments and web-based applications.

Gain industry-leading cloud capabilities in a flexible, subscription-based format.

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.

Cisco Response:

Read and understood. Our auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

6.5 (E) BILLING AND PRICING PRACTICES

DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

[8] Cisco Powered cloud services: http://www.cisco.com/web/solutions/trends/cisco-powered/index.html

Cisco Response:

Cisco Cloud services billing is broken down into the following:

- Fixed cost — Specific per virtual machine instance costs such as floor space, power/cooling, software or administrative overhead.
- Allocation-based costing — Variable costs per virtual machine based on allocated resources, such as the amount of memory, CPU or storage allocated or reserved for the virtual machine in VMware vCenter Server.
- Utilization-based costing — Variable costs per virtual machine based on actual resources used, including average memory, disk and CPU usage, network I/O and disk I/O.

The mediation engine collects the usage data, which can be the one or more of the following:

- Netflow
- APIs
- FTP
- SNMP

Tickets or CDRs (Call Detailed Records) are generated based on the collected information and sent to the rating engine for further processing. Rating involves the identification of the subscriber's service and allocation of a price for the service usage. Each customer's bill is then generated based on the rating and usage details collected and processed.

Rating and charging could be based on:

- Individual usage, i.e. each collected usage record is rated individually and delivered to billing or other BSS
- Aggregated usage over longer period of time, such as 95-percentile sampling
- SLA Management and Service Assurance.

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement the your cloud solutions.

Cisco Response:

Cost impacts vary widely across the various cloud services, especially comparing IaaS from SaaS. For our typical SaaS offerings, cost impacts might be related to integration with other existing customer infrastructure. For our Metapod private IaaS offering, cost impacts might include application migration planning, infrastructure assessments, etc. Cisco will work with any purchasing entity to identify any potential cost impacts, if any.

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.

Cisco Response:

All of the proposed Cisco cloud offerings are compliant and offered per the applicable service model based on NIST 800-145. As part of our technical response, each of the offerings are described in how they meet the five essential characteristics of Cloud Computing, as well as how they meet the NIST service and deployment model definitions.

6.6 (E) SCOPE AND VARIETY OF CLOUD SOLUTIONS

Specify the scope and variety of the Solutions you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services and deployment models that you offer.

Cisco Response:

Cisco offers a broad set of capabilities that help you meet the unique needs of the various government users and organization functions. Because one size does not fit all when determining the type of cloud service and its applicable deployment model, Cisco has developed cloud solutions that encompass infrastructure as well as applications in various categories of services including:

- Collaboration
  - ❑ WebEx
  - ❑ Spark
  - ❑ Tropo
- Security
  - ❑ Cloud Email Security
  - ❑ Cloud Web Security
- Infrastructure
  - ❑ Metapod
  - ❑ Meraki
  - ❑ Energy Management
  - ❑ Cloud Consumption as a Service.

Table 4 lists the offering, service model, deployment model, and data classification levels for each.

Table 4. Offering Service Model, Deployment Model, and Data Classification Levels

Cisco Offering	Service Model	Deployment Model	Data Classification Levels
Metapod	IaaS	Private	L, M
WebEx	SaaS	Public, Community	L, M
Spark	SaaS	Public	L, M
CES	SaaS	Private	L, M
CWS	SaaS	Public	L
Meraki	SaaS	Public, Hybrid	L

Cisco Offering	Service Model	Deployment Model	Data Classification Levels
Tropo	PaaS	Public	L, M
Energy Management (CEM)	SaaS	Public	L
Cloud Consumption as a Service	SaaS	Public	L

6.7 (E) BEST PRACTICE

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.

Cisco Response:

Cisco information security policies are designed to meet the ISO/IEC 27001 Information Security Management Systems (ISMS) requirements and are available on the Cisco intranet to all employees, contractors, consultants, temporary, and other workers at Cisco. In certain cases, Cisco has implemented more stringent internal controls to comply with legal, regulatory, or customer security requirements.

Organizational Profile

7 ORGANIZATION AND STAFFING

(ME) 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 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.

Cisco Response:

Name: Mimi Nguyen-Farr

Phone: (408) 527-2627

Email: mimnguye@cisco.com

Working Hours: 9 a.m. to 5 p.m. PST

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.**

Cisco Response:

Mimi's experience consists of 8+ years in the Data Communications Services Business and 21+ years in High Tech Contracts Negotiations and Management. An overview of the contract management expertise can be found in Attachment 11 NVP Cloud_Cisco Response_MFarrResume Mar2016. She has a team of 10 professionals who are solely responsible for contracts management, administration and compliance of Cisco's direct State, Local Governments, and Education contracts across the U.S.

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.

Cisco Response:

Ms. Mimi Nguyen-Farr, Sr. Manager, will be the single point of contact and responsible for general oversight of the new NASPO ValuePoint Master Agreement, including the following key functions:

- Participate in the contract negotiations as a business lead with Cisco Legal after contracts award;
- Lead the efforts to operationalize and implement the new contract and each Participating Addendum that gets executed;
- Drive the vetting, selection and onboarding of the selected Resellers for each Participating Addendum;

- Develop and maintain contract webpages for the Master Agreement and each Participating Addendum;
- Oversee the submission of the quarterly usage reports and applicable administrative fees for both the Master Agreement as well as each Participating Addendum;
- Ensure other contractual and compliance obligations are met (i.e., E-Verify, Certificate of Insurance, etc.), including providing mandatory trainings to the authorized resellers, and Cisco Sales, and webinars for those authorized customers under the Participating Addendums;
- Conduct annual performance reviews of the authorized resellers under each Participating Addendum; and
- Facilitate marketing campaigns to increase adoption and usage of the new contract and Participating Addendums.

Technical Response

Cisco has fully read, understood, and analyzed the Request for Proposal (RFP) for Cloud Solutions. Based on the RFP requirements, Cisco has proposed Cloud Solutions that meet every NIST Cloud Service Model (IaaS, SaaS, and PaaS) in various NIST Deployment Models. The Cisco Cloud Portfolio is built on validated architectures, innovative infrastructure solutions, and best practices to help IT organizations become a trusted broker of IT services, plan their journey to the cloud, and get there quickly and efficiently. We believe this combination provides the most secure, scalable, and highest performance of cloud solutions in the industry, since most Cisco validated architectures are built to provide 99.99 percent type SLAs with the highly regarded Cisco Technical support available 24X7X365.

The Cisco Cloud Solutions to be provided are based on various subcategories such as:

- Collaboration
- Infrastructure
- Security.

8 TECHNICAL REQUIREMENTS

If applicable to an Offerors offering, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's offering then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8.1 (M)(E) 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.**

Cisco Response:

Cisco Cloud — Flexible Consumption Choices

A rich variety of cloud consumption models are available. Cisco offers a comprehensive set of market-leading technologies and services for faster IT and cloud innovation. Using our experience working with many customers worldwide, we can help you build and manage your cloud deployment. Our solutions combine our extensive experience, knowledge, and best practices with our constantly expanding portfolio of cloud offerings (**Table 5**). Cisco also has a nationwide staff of Cisco employees certified in Consulting Services available to help provide the resources the State might need in planning, designing, implementing, or monitoring their cloud strategy, services, and infrastructure.

Table 5. A Diverse Array of Cisco Cloud Models Available to Meet Specific Needs

Cisco Cloud Offering	Cloud Service Model	Deployment Models	Location
Metapod	IaaS	Private, Hybrid	Customer Premises
WebEx	SaaS	Public, Community	Service Provider
Spark	SaaS	Public	Service Provider
Cloud Email Security	SaaS	Hybrid	Service Provider
Cloud Web Security	SaaS	Hybrid	Service Provider
Meraki	SaaS	Hybrid	Service Provider
Tropo	PaaS	Public	Service Provider
Cisco Energy Management	SaaS	Public	Service Provider
Cloud Consumption as a Service	SaaS	Public	Service Provider

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.

Cisco Response:

Table 6. NIST Characteristic - On-Demand Self-Service

Cisco Cloud Offering	Response
Metapod	Users accessing Metapod dashboard can provision virtual machines (server time in NIST terminology), storage volumes, and network resources in a self-service mode (without having to interact with administrators).the provisioning process is 100 percent automatic with no manual process required by a cloud platform admin. Resources are provisioned on demand (there is no pre-provisioning) and de-provisioned once there is no need for them anymore.
WebEx	The Cisco WebEx Service High Availability (SHA) team is dedicated to maintain the availability of Cisco WebEx services. Weekly Capacity Monitoring meetings are held to monitor trends of network and server usage and identify needs for cluster

Cisco Cloud Offering	Response
	expansion without customer having to worry about it.
Spark	The Spark application meets all the essential characteristics published within the NIST Special Publication 800-145. Spark is a software application that sits on top of Cisco’s private infrastructure. Cisco provisions computing capabilities, such as server time and network storage, automatically by the Spark application without requiring human interaction.
Cloud Email Security	CES is provisioned after contract by Cisco and is available to designated customers. Customers have a dedicated service per customer and can manage and configure each email security server per their unique requirements. Customers have control over service policy and configuration variables using a dedicated portal provided exclusively for their use.
Cloud Web Security	CWS is provisioned after contract by Cisco and is available to designated customers. Customers have a dedicated access per customer and can manage and configure service policy per their unique requirements. Customers have control over service policy and configuration variables using a portal provided for their use.
Meraki	Once a customer purchases a Meraki product, they simply go to dashbaord.meraki.com, create an account, and claim their order number. From there, they can configure their purchase in the cloud, claim additional purchases, or create additional administrator accounts.
Tropo	The Tropo application meets all the essential characteristics published within the NIST Special Publication 800-145. Tropo is a software application that sits on top of Cisco’s private infrastructure. Cisco provisions computing capabilities, such as server time and network storage, automatically by the Tropo application without requiring human interaction.
Cisco Energy Management	Use this Software-as-a-Service (SaaS) application to manage energy without hosting the Cisco Energy Management application in your data center. Reduce energy usage and gain complete visibility without having to purchase, provision, or maintain expensive servers. Pay as you grow, with convenient 1-, 3-, or 5-year subscriptions.
Cloud Consumption as a Service	The Cloud Consumption as a Service (CCaaS) application meets all the essential characteristics published within the NIST Special Publication 800-145. CCaaS is a software application that sits on top of Cloud IaaS (Private). Cisco provisions computing capabilities, such as server time and network storage, automatically by the CCaaS application without requiring human interaction. Also, CCaaS can be accessed at any time and from anywhere with the possibility of customization (on-

Cisco Cloud Offering	Response
	demand self-service). All of the features provided by CCaaS are supported by the majority of web browsers (broad network access). Cisco may use a shared pool of resources (compute, network, storage, etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the CCaaS application demand (Resource pooling). The Cisco Cloud Infrastructure which hosts the CCaaS application may have its capabilities elastically provisioned and released. In some cases, this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from CCaaS application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer. The CCaaS application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts the CCaaS) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service).

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.

Cisco Response:

Table 7. NIST Characteristic - Broad Network Access

Cisco Cloud Offering	Response
Metapod	Metapod service is accessed by users via dashboard (web interface), APIs, or CLI. All these methods of access are based on TCP/IP and users can access them as long as they have a TCP/IP connection to the Metapod deployment (and they have proper access throughout the network).
WebEx	Broad Network access is through a URL meeting invitation link that is available to meeting attendee over commonly available platforms for computers and mobile devices.
Spark	The Spark application meets all the essential characteristics published within the NIST Special Publication 800-145. Spark is a software application that sits on top of Cisco's private infrastructure. Cisco provisions computing capabilities, such as server time and network storage, automatically by the Spark application without requiring human interaction.
Cloud Email Security	CES service is available on SMTP, SMTP over TLS, and S/MIME protocols. Customer email is directed using published Internet DNS standard records and data center secure gateways and firewalls. Service is available worldwide, irrespective of customer location.

Cisco Cloud Offering	Response
Cloud Web Security	CWS is available over HTTP and HTTPs protocols. Service is forwarded to the CWS Cloud using specific IP address and authentication keys unique to each customer for authentication and authorization of forwarded traffic. Service is available worldwide, irrespective of customer location.
Meraki	Customers access the Cisco Meraki Dashboard by logging in at dashbaord.meraki.com. Security mechanisms exist to protect that login, including two-factor authentication, mandatory password length or age, idle log-out, etc.
Tropo	The Tropo application meets all the essential characteristics published within the NIST Special Publication 800-145. Tropo is a software application that sits on top of Cisco's private infrastructure. Cisco provisions computing capabilities, such as server time and network storage, automatically by the Tropo application without requiring human interaction.
Cisco Energy Management	CEM provides a web-based interface that allows facilities and network management applications to communicate with endpoints and each other, using the network as a unifying fabric. The Cisco EnergyWise Suite provides a framework by which the network itself can be used to open power management to all device types, including integration with Building Management Systems (BMS). The Cisco EnergyWise Suite provides flexible and unified policy management across device and vendor type.
Cloud Consumption as a Service	The Cloud Consumption as a Service (CCaaS) application meets all the essential characteristics published within the NIST Special Publication 800-145. CCaaS is a software application that sits on top of Cloud IaaS (Private). Cisco provisions computing capabilities, such as server time and network storage, automatically by the CCaaS application without requiring human interaction. Also, CCaaS can be accessed at any time and from anywhere with the possibility of customization (On-demand self-service). All of the features provided by CCaaS are supported by the majority of Web Browsers (Broad network access). Cisco may use a shared pool of resources (compute, network, storage etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the CCaaS application demand (Resource pooling). The Cisco Cloud Infrastructure which hosts the CCaaS application may have its capabilities elastically provisioned and released. In some cases this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from CCaaS application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer. The CCaaS application

Cisco Cloud Offering	Response
	performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts the CCaaS) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)

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.

Cisco Response:

Table 8. NIST Characteristic - Resource Pooling

Cisco Cloud Offering	Response
Metapod	Metapod aggregates all physical compute, network, and storage resources as pools and presents them as pools of virtual resources to the users. Users are organized in tenant and access to the resources is managed based on user and tenant. Virtual resources (VMs, internal IP addresses, storage volumes, etc.) are assigned dynamically based on user demand. Users have access to these virtual resources without having knowledge on where the physical resources used are located.
WebEx	Cisco WebEx Cloud Collaboration service WebEx is a SaaS environment and does not support dedicated resources for each tenant/customer. The environment is designed to support customer/tenants based on industry practices.
Spark	The Spark application meets all the essential characteristics published within the NIST Special Publication 800-145. Cisco may use a shared pool of resources (compute, network, storage etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the Spark application demand (Resource pooling).
Cloud Email Security	Resource pooling is managed at the hardware, network, and data center layers. Customers retain individual virtual device administration capabilities. Service is provided for multiple tenants, but each tenant is uniquely defined and managed using a separate instance of Cisco's industry leading Email Security Appliance software.
Cloud Web Security	Resource pooling is managed at the application, network, machine, hardware, and data center layers with redundant peer connections to the public Internet.
Meraki	Cisco Meraki is a multi-tenant cloud. Resources are automatically pooled by Meraki to service all customers and all devices under management.

Cisco Cloud Offering	Response
Tropo	The Tropo application meets all the essential characteristics published within the NIST Special Publication 800-145. Cisco may use a shared pool of resources (compute, network, storage etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the Tropo application demand (Resource pooling).
Cisco Energy Management	Not applicable for this service.
Cloud Consumption as a Service	The Cloud Consumption as a Service (CCaaS) application meets all the essential characteristics published within the NIST Special Publication 800-145. CCaaS is a software application that sits on top of Cloud IaaS (Private). Cisco provisions computing capabilities, such as server time and network storage, automatically by the CCaaS application without requiring human interaction. Also, CCaaS can be accessed at any time and from anywhere with the possibility of customization (On-demand self-service). All of the features provided by CCaaS are supported by the majority of Web Browsers (Broad network access). Cisco may use a shared pool of resources (compute, network, storage etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the CCaaS application demand (Resource pooling). The Cisco Cloud Infrastructure which hosts the CCaaS application may have its capabilities elastically provisioned and released. In some cases this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from CCaaS application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer. The CCaaS application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts the CCaaS) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)

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.

Cisco Response:

Table 9. NIST Characteristic - Rapid Elasticity

Cisco Cloud Offering	Response
Metapod	Resources are allocated either manually (dashboard, CLI) or automatically (CLI scripting or APIs); therefore, the capacity of

Cisco Cloud Offering	Response
	resources can elastically scale up and down and it appears unlimited to the user.
WebEx	The Webex application meets all the essential characteristics published within the NIST Special Publication 800-145. Rapid elasticity capabilities are achieved by the Cisco WebEx Service High Availability feature during monitoring and expansion of storage or network capacity through virtualization.
Spark	The Cisco Cloud Infrastructure which hosts the Spark application may have its capabilities elastically provisioned and released. In some cases this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from the Spark application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer.
Cloud Email Security	CES is relatively inelastic in the NIST-defined sense of the term. Cisco Data Center personnel manage customers' resources and SMTP traffic is processed and queued for delivery based on resources assigned. Additional resources can be allocated for customer use by customer request.
Cloud Web Security	CWS is highly elastic and will scale to meet customer HTTP and HTTPS request traffic.
Meraki	Customers can manage an unlimited number of devices in the Meraki cloud. We have single customers with over 100,000 devices under management. Customers are free to add as many devices as they like at any given time. Meraki's cloud dashboard is designed to be very lightweight and Cisco Meraki automatically monitors the status of the compute infrastructure supporting our customers and scales up as necessary without impacting customer's environments.
Tropo	The Cisco Cloud Infrastructure which hosts the Tropo application may have its capabilities elastically provisioned and released. In some cases this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from the Tropo application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer.
Cisco Energy Management	Not applicable for this service.
Cloud Consumption as a Service	The Cloud Consumption as a Service (CCaaS) application meets all the essential characteristics published within the NIST Special Publication 800-145. CCaaS is a software application that sits on top of Cloud IaaS (Private). Cisco provisions

Cisco Cloud Offering	Response
	computing capabilities, such as server time and network storage, automatically by the CCaaS application without requiring human interaction. Also, CCaaS can be accessed at any time and from anywhere with the possibility of customization (On-demand self-service). All of the features provided by CCaaS are supported by the majority of Web Browsers (Broad network access). Cisco may use a shared pool of resources (compute, network, storage etc.) using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the needs of the CCaaS application demand (Resource pooling). The Cisco Cloud Infrastructure which hosts the CCaaS application may have its capabilities elastically provisioned and released. In some cases this is done automatically in order to scale rapidly outward and inward - commensurate with demand coming from CCaaS application. The capabilities available for provisioning are unlimited and can be allocated in any quantity and at any time, but all these are transparent to the customer. The CCaaS application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts the CCaaS) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)

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.

Cisco Response:

Table 10. NIST Characteristic - Measured Service

Cisco Cloud Offering		Response
Metapod		Metapod provides reports to both the users and administrators on use of key resources (cpu, memory, and disk). Users get a view of their project and usage against quota, administrators get a view of the overall utilization on a per-tenant basis. Custom reports can be run for specific time periods. We also offer cloud metrics, which gives you a graphical view over time of key resources. The Metacloud capacity monitoring will also help NASPO ensure maximum utilization of hardware resources. Detailed usage reports provided by Cisco Metapod can be further delivered as input

Cisco Cloud Offering		Response
		into show-back or charge-back (or billing) applications like Cloud Cruiser, StackOps, Amysta Charge-Back, CloudKitty, etc.
WebEx		Cisco WebEx is a Software as a Service subscription-based model based on activity usage.
Spark		The Spark application meets all the essential characteristics published within the NIST Special Publication 800-145. The Spark application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts Spark) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)
Cloud Email Security		Cisco Security Operations personnel measure CES service internally. Monitoring control and management are accomplished using industry standard tools and protocols and best practice methodology. Reports relating application performance are available to client customers; other reports are available to systems operations and SOC personnel.
Cloud Web Security		Cisco Security Operations personnel measure CWS service internally. Monitoring control and management are accomplished using industry standard tools and protocols and best practice methodology. Reports relating application performance are available to client customers; other reports are available to systems operations and SOC personnel.
Meraki		Customers purchase licenses for the Cisco Meraki cloud. These licenses entitle customers to manage network components in the cloud. On the licensing screen in the Meraki dashboard, customers can see their current licensing limit, how many of these licenses they are currently using, and what their renewal date is.
Tropo		The Tropo application meets all the essential characteristics published within

Cisco Cloud Offering		Response
		the NIST Special Publication 800-145. The Tropo application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts Tropo) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)
Cisco Energy Management		Not applicable for this service.
Cloud Consumption as a Service		The Cloud Consumption as a Service (CCaaS) application meets all the essential characteristics published within the NIST Special Publication 800-145. The CCaaS application performance is monitored. Also, resources for the Cisco Cloud IaaS (that hosts the CCaaS) can be monitored, controlled, and reported, and it provides transparency for both the provider and consumer of the utilized service (measured service.)

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.

Cisco Response:

Cisco is pleased to offer a strong combination of NIST-compliant service models in all three areas of IaaS, SaaS, and PaaS. Our breadth of secure, high-performance infrastructure cloud solutions is from Infrastructure offerings such as a Private Managed Cloud to SaaS, offering such as the #2 largest SaaS offering, WebEx.

Our offerings can be classified as the following service models with subcategories provided for our vast SaaS offerings. **Table 11** lists our service model, subcategories, and description.

Table 11. Service Models with Subcategories

Service Model	Subcategories	Cisco Offering	Cisco Offering Description
IaaS	NA	Metapod	Private, Hybrid Managed Cloud — On customer premises
PaaS	NA	Tropo	API as a service platform
SaaS	Collaboration	WebEx	Web conferencing as a service
SaaS	Collaboration	Spark	Next generation collaboration
SaaS	Security	Cloud Email Security	Email security as a service
SaaS	Security	Cloud Email Security	Web site security as a service
SaaS	Infrastructure	Meraki	Wi-Fi management as a service
SaaS	Infrastructure	Cisco Energy Management	Energy management as a service.
SaaS	Infrastructure	Cloud Consumption as a Service	Cloud discovery as a service

8.1.4 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.

Cisco Response:

Cisco is willing to comply with the requirements of Attachments C and D.

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**.

Cisco Response:

Table 12. Services Definitions, Deployment Model, and Data Classification

Cisco Offering	Service Model	Deployment Model	Data Classification Levels
Metapod	IaaS	Private	L, M
WebEx	SaaS	Public, Community	L, M
Spark	SaaS	Public	L, M
CES	SaaS	Private	L, M
CWS	SaaS	Public	L
Meraki	SaaS	Public, Hybrid	L
Tropo	PaaS	Public	L, M
Energy Mgt (CEM)	SaaS	Public	L
Cloud	SaaS	Public	L

Cisco Offering	Service Model	Deployment Model	Data Classification Levels
Consumption			

8.2 (E) SUBCONTRACTORS

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. Subcontractor do not need to comply with Section 6.3.

8.2.1 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.

Cisco Response:

Subject to Cisco's provisioning and delivery of each of its offerings, Cisco, however, utilizes a reseller model for actual sales and order fulfillment/processing. Consistent with the current process under Cisco's existing NASPO ValuePoint Data Communications AR233 (14-19) Master Agreement, Cisco wishes to defer the selection of these "Authorized Resellers" (subcontractors) until after contract award and upon execution of each Participating Addendum. Notwithstanding the foregoing, Cisco may allow these Authorized Resellers to offer limited value–added services initially as set forth in Attachment G- Cost Schedule such as basic installation and configuration services. However, Cisco may also allow the Authorized Resellers to offer "CMSP Services" as described in Cisco's redlines to the Terms and Conditions of the Master Agreement later on after contract award. CMSP Services shall mean in scope offerings which may be provided by an Authorized Reseller, which are running on Contractor-powered infrastructure and based on Cisco's recommended and validated architectures. As such CMSP Service offerings become available, the parties may add such offerings by amending the awarded contract as mutually agreed upon by both parties. Cisco understands and agrees that any Authorized Reseller (subcontractor) that it 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.

8.2.2 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.

Cisco Response:

As stated above, Cisco wishes to defer the selection of these "Authorized Resellers" (subcontractors) until after contract award and upon execution of each Participating Addendum. However, Cisco will employ the following strategic qualifying and selection process of Authorized Resellers for each executed Participating Addendum:

Cisco understands and is sensitive to the fact that not all our resellers have the capacities to sell in every state across the U.S. Many are small to medium businesses who are focused in selling and supporting certain geographic areas, technology practice and/or type of Public Sector customer(s) (i.e. state agencies, K-12, etc.). Therefore, to ensure the engagement and participation of diverse resellers, including "local" businesses, our reseller selection process aims to objectively select multiple resellers that can best serve the needs of the Participating Entities identified in each Participating Addendum:

- Cisco will solicit input from the Participating State who executed a Participating Addendum (i.e. State of X) on its specific needs and/or requirements (i.e. local presence, certain technology cloud expertise, area coverage, etc.).
- Based on the Participating State's input and Cisco's own business criteria and requirements, Cisco will follow its established process for soliciting and selecting appropriately skilled authorized resellers.
- Selected resellers will be expected to (i) "pass" Cisco's legal and financial due diligence checks, and (ii) execute a subcontract with Cisco and adhere to the terms and conditions of the resulting new contract as well as the respective Participating Addendum.

Our application and selection process takes into account, but not limited to, the following considerations in selecting the resellers that will be authorized to sell to the customer base identified in each Participating Addendum:

- Physical presence within the state (economic development, customer access, etc.);
- Geographic coverage (i.e. north, central, south, remote areas, etc.)
- Reseller's Cisco certification level and cloud specializations in order to meet the requirements of the RFP;
- Cisco certified engineering and trained sales staff;
- Proven historical public sector sales experience and success in the state or geographic location/territory as identified in the Participating Addendum; and
- Other value added services that Cisco and/or the Participating Entity may require under that Participating Addendum.

All Authorized Resellers will be required to execute a subcontracting agreement with Cisco that will include the flow downs of the terms and conditions of the RFP and Master Agreement as well as the applicable Participating Addendum(s) to ensure compliance of all requirements. These contractual obligations will also apply and be incorporated into to all Statements of Work that the Authorized Resellers may execute with the Participating Entities.

8.3 (E) 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.

Cisco Response:

Purchasing Entity identified contact will be notified in 48 hours of a confirmed breach by the Incident Commander in writing or as specified in the contract. The Data Protection and Privacy team within Cisco's Security and Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging the talents of diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

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.

Cisco Response:

Cisco will not market or sell the Participating Entity's information nor does it allow for any adware, software, or marketing material in its content. Cisco also employs standard data center security best practices to block adware, malware, and other unwanted intrusions.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Cisco Response:

The Cisco Cloud solutions offered as part of this proposal support a testing/environment that is nearly identical to production. Where applicable (IaaS), customers are allowed to run a more customer-specific trial on premises.

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.

Cisco Response:

The Cisco Cloud solutions offered as part of this proposal are accessible by people with disabilities. Certain products may require third-party add-ons.

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.

Cisco Response:

Table 13. Web Browsers Supported

Cisco Cloud Offering	Response
Metapod	Cisco Metapod is compatible with Firefox and Firefox ESR (version 31), Chrome (43.0.2357.81) and Internet Explorer (version 11+). Other browsers are most probably compatible but were not specifically tested.
WebEx	Supported browsers include: Internet Explorer 7, 8, 9, 10, 11 (all 32 bit/64 bit); Firefox (Latest); Safari 5, 6, 7, 8; Chrome (32 bit/64 bit for Windows

Cisco Cloud Offering	Response
	and Mac OS).
Spark	Yes, Spark is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Cloud Email Security	CES is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Cloud Web Security	CWS is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Meraki	Yes, the Cisco Meraki Dashboard is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Tropo	Yes, Tropo is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Cisco Energy Management	CEM is accessible through Internet Explorer, Firefox, Chrome, and Safari.
Cloud Consumption as a Service	CCaaS is being supported by all the major web browsers (i.e., Firefox, Safari, Chrome)

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.

Cisco Response:

Cisco will 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 Cisco that is subject to any law, rule, or regulation providing for specific compliance obligations.

8.4 (E) 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).

Cisco Response:

For customers with current Cisco service contracts, Cisco provides technical support services 24 hours per day, 7 days per week, on the web and over the phone.

The following escalation management plan is currently in place today for the purpose of timely addressing any contractual issues and/or concerns raised by our NASPO ValuePoint customers.

- **Review and Appropriate Escalation.** Upon notification of an issue or concern by a customer and after performing the necessary review and investigation, Cisco's U.S. Public Sector Contracts Management Office (CMO) will lead the effort to properly communicate the matter to the appropriate internal and external stakeholders for action, including senior management of all parties involved as necessary. For example, issues may be escalated to Cisco management in Sales, Channels, Legal, Finance, and/or other impacted Cisco department(s) as required to properly evaluate and address the issue or concern. If the matter is related to one of its Authorized Resellers, Cisco's CMO will also reach out to that Authorized Reseller and its management sales team accordingly.
- **Corrective Actions.** Depending on the nature of the issue, the appropriate corrective actions within Cisco's control will be identified and implemented as Cisco deems necessary or commercially reasonable to execute in order to ensure satisfactory resolution. Cisco's CMO will keep State of Utah and/or the Participating State or Entity apprised of its progress. Where the corrective action requires involvement or engagement of external parties, Cisco's CMO will follow up with such parties appropriately.
- **Feedback and Continuous Process Improvement.** Cisco's CMO welcomes and encourages regular feedback from all of its NASPO ValuePoint customers as it continuously strives to maintain operational excellence and customer satisfaction. In addition, Cisco's CMO may also make recommendations for process improvements based on lessons learned and will work with the State of Utah and the Participating State or Entity (as applicable) on such initiatives, as appropriate.

Cisco will continue to follow this escalation management plan for the new NASPO ValuePoint contract, subject to any continuous process improvements that Cisco may implement.

8.4.2 Offeor 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.

Cisco Response:

In addition to Cisco's response to Section 8.4.2(b) below, Cisco will also maintain a dedicated contract web page at www.Cisco.com for each executed Participating Addendum, which will include key contact information of the Cisco team members assigned for that Participating State or Entity. Generally, the Regional Manager or Account Manager for the Participating State will be designated as the lead representative.

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.

Cisco Response:

For customers with current Cisco service contracts, Cisco provides technical support services 24 hours per day, 7 days per week, on the web and over the phone.

Technical Related Issues. When a customer purchases SMARTnet and/or any of Cisco's Technical/Maintenance Services, the customer will have access to the Cisco Technical Assistance Center (TAC). TAC has a formal process in place for handling and responding to customer case-escalation requests. To help ensure all service requests are reported in a standard format, TAC has established the following service request severity definitions, as shown in **Table 14**.

Table 14. Service Request Severity Definitions

Severity Level	*Definition*
Severity 1 (S1)	Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit considerable resources around the clock to resolve the situation.
Severity 2 (S2)	Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected. You and Cisco will commit considerable resources during normal business hours to resolve the situation.
Severity 3 (S3)	Operational performance of your network is impaired, while most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
Severity 4 (S4)	You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

If you feel that progress on your service request or the quality of Cisco Services is not satisfactory, Cisco encourages you to escalate the service request. You can do this by contacting the TAC and asking for the TAC duty manager. Online resources and phone numbers for contacting the appropriate Cisco TAC are available at: http://www.cisco.com/en/us/support/tsd_cisco_worldwide_contacts.html

As part of ISO standards for escalation process workflow, email alerts are generated by the TAC trouble ticketing system, notifying the individuals listed in **Table 15** if no activity (update or status change) is recorded against a service request for the following periods. Severity 1 alert times are measured in calendar hours — 24 hours per day, 7 days per week. Severity 2 alert times corresponds with standard business hours.

Table 15. Automatic Email Alert Escalations for Cisco TAC Service Requests

	Severity 1 ***Network Down***	***Severity 2*** ***Severe Impact***
1 Hour	TAC Manager	
4 Hours	TAC Director	TAC Manager
24 Hours	VP Customer Advocacy	TAC Director
48 Hours	President	VP Customer Advocacy
96 Hours		President

Continuous improvement in service quality is driven and measured by the use of customer satisfaction surveys. Cisco uses both relationship and transactional surveys to identify strengths and opportunities for improvement. Organizational, management, and individual goals and objectives are established based on the results of these surveys. Improvement plans are developed based on the key messages from the surveys and progress is tracked and reported at monthly and quarterly reviews.

c. Customer Service Representative will respond to inquiries within one business day.

Cisco Response:

Read and understood. In addition, please see Cisco's response to Section 8.4.2(b) above.

d. You must provide design services for the applicable categories.

Cisco Response:

Read and understood. Design Services will be available for customers to purchase under the awarded contract. Customers will have the option to have the delivery of those Design Services performed by Cisco and/or its Authorized Resellers under each Participating Addendum.

e. You must provide Installation Services for the applicable categories.

Cisco Response:

Read and understood. Installation Services will be available for customers to purchase under the awarded contract. Customers will have the option to have the delivery of those Installation Services performed by Cisco and/or its Authorized Resellers under each Participating Addendum.

8.5 (E) 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.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

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.

Cisco Response:

Table 16. Security of Information

Cisco Cloud Offering	*Response*
Metapod	**General** Deploying a private managed cloud creates a shared responsibility model between the customer and Cisco. We take security, confidentiality, and trust very seriously and use industry best practices to ensure we deliver on those critical elements. Our controller nodes are secure and hardened and adhere to the best practices for securing UNIX/Linux systems, which includes turning off un-needed services, network ports, and daemons. The Cisco OpenStack solution will adhere to the Customer Security Alignment requirements. Cisco works very closely with its clients to understand their security policies, network architecture, and overall data center operational practices. We then work closely to fit our solution within the security policies of our clients. When we deploy a private cloud for a client, we document the design, the security and access policies, and take full responsibility for our monitoring and access auditing of these systems. As with most private clouds, network security and privacy is critical and Cisco deployments are typically within a customer's existing network environment, behind their network firewall, using their security access methods. Cisco Metapod uses VLANs in its design with strict security and access between different tenants. Our VLANs take advantage of 802.1Q VLAN tagging to secure our networks from one another. Our system supports an administration role that can control users, quotas, and authentication, as well as oversee all accounting on a per-tenant basis. The accounting can be seen in the overview option of the project/tenant menu. Information security, process, and procedure controls are important components in the Cisco Managed Service offering. Cisco's development processes and systems environment are based upon industry best practices, and audits are regularly conducted using technologies such as Qualys Systems security scans. **Application Isolation** Cisco Metapod IaaS service supports authenticating against Active Directory, LDAP, and local accounts, allowing our clients to leverage their existing user accounts. Additionally, while user authentication can be done against Active Directory, LDAP, or local accounts, authorizations are stored in Keystone, the OpenStack identity provider, allowing customers to get started immediately without needing to make complicated

Cisco Cloud Offering	Response
	schema modifications to their directory services. The identity service within Cisco OpenStack provides a central directory of users mapped to the various services they can access and is also the foundation for preventing unauthorized access. It acts as a common authentication system across the cloud operating system and can integrate with existing back-end directory services like LDAP. It supports multiple forms of authentication, including standard username and password credentials, token based systems, and AWS-style logins. Additionally, the catalog provides a queryable list of all of the services deployed in the cloud in a single registry. Users and third-party tools can programmatically determine which resources they can access. Within the platform, identities can either be managed entirely within the environment, or can integrate with external protocols like LDAP or Active Directory. This allows you to maintain the benefits of your existing mature, audited account management system, with no need for duplication of workflows. The ownership of the data rests with each of our clients, as well as the security and recovery of the data. Our solution contains many security features to assist in building a secure cloud, including firewalls, security groups, public-private key pairs, floating IPs as well as methods to “snapshot” or “backup” instances. The management of the virtual machines, application, application data, security, and backup or recovery, however, is ultimately a client responsibility. To maintain maximum flexibility, customers can choose to use an external encryption key management system of their choice. As per the service description, this function is in the customer scope of responsibilities. Cisco continues to track and contribute to OpenStack features such as Barbican. When extensions like these evolve, they will be candidates for integration into the platform. **Authorization** Cisco uses Keystone for authorization and authentication. We support all use cases of Keystone. We support internal directory to Keystone, Active Directory, and LDAP: ■ LDAP Simple store for VM, tenants, and users ■ LDAP Guest Access ■ LDAP Cloud Operator ■ LDAP Proxy to authenticate against a remote LDAP includes windows image and guest ■ LDAP Proxy with windows image and guest ■ AD backend ■ AD join Domain + Domain Auth

Cisco Cloud Offering	Response
	■ AD Tenant plus restrictions ■ AD Cloud Operator ■ AD Delegation with tenants **Role-Based Access and Governance** Cisco supports authenticating against Active Directory, LDAP, and local accounts, allowing our clients to leverage their existing user accounts. Additionally, while user authentication can be done against Active Directory, LDAP, or local accounts, authorizations are stored in Keystone, the OpenStack identity provider, allowing you to get started immediately without needing to make complicated schema modifications to your directory service. The Identity service within Cisco OpenStack provides a central directory of users mapped to the various services they can access and is also the foundation to prevent unauthorized access. It acts as a common authentication system across the cloud operating system and can integrate with existing backend directory services like LDAP. It supports multiple forms of authentication including standard username and password credentials, token-based systems, and AWS-style logins. Additionally, the catalog provides a queryable list of all of the services deployed in the cloud in a single registry. Users and third-party tools can programmatically determine which resources they can access. Within the platform, identities can either be managed entirely within the environment, or can integrate with external protocols like LDAP or Active Directory. This allows you to maintain the benefits of your existing mature, audited account management system, with no need for duplication of workflows. Cisco has enhanced the user interface of the Horizon dashboard and provides the cloud administrator much greater control to manage a large number of hypervisor systems and multiple availability zones. Our system provides reports to both the users and admin on use of key resources (CPU, memory, and disk). Users get a view of their project and usage against quota; administrators get a view of the overall utilization on a per-tenant basis. Custom reports can be run for specific time periods. We also offer cloud metrics, which gives you a graphical view over time of key resources. Cisco supports an administration role that can control users, quotas, authentication, and overall see accounting on per-tenant basis. The accounting can be seen in the overview option of the project/tenant menu. In addition, we support project-based administration through our own self-service enhancement, which means a user can become the administrator of their own project and control access to those resources. When combined

Cisco Cloud Offering	Response
	with Active Directory or LDAP integration, it can provide a zero-touch self-service environment for your users. **VM Security** Our cloud solution implements OpenStack security groups, which can be used to customize or standardize VM security per the customer's security standards. It is up to the administrator or tenant owner to establish these standard security rules and then make them available to the users. **CSA Security Control** Information security, process, and procedure controls are important components in the Cisco Managed Service offering. Cisco's development of security processes and systems is based upon industry best practices, and audits are regularly conducted using technologies such as Qualys Systems security scans. These audits are generally done by our clients because the solution site is their data center. Please see the attached Security White Paper for additional information on security practices. **Hardening/Compliance Check/Vulnerability Assessment** Since the on-prem cloud is deployed within a client's IT framework, all of their security practices would apply from a network and external firewall perspective. We also provide tools to place firewall rules on VMs within the cloud through OpenStack security groups, for another layer of security. Cisco can also work with the customer to architect the best solution to meet any intrusion detection and/or prevention demands. We have hardware and software based intrusion detection and prevention apparatus, plus managed service offerings from Sourcefire, a Cisco entity. We will work with the customer to architect the best and most accommodating solution to address the need and its management challenges. **Encryption** To maintain maximum flexibility, customers can choose to use an external encryption key management system of their choice. As per the service description, this function is in the customer scope of responsibilities. Cisco continues to track and contribute to OpenStack features such as Barbican. When extensions like these evolve, they will be candidates for integration into the platform. **Data Access** Client data is generally stored within the guest operating system instance, which is owned and managed by the client. The security set at the instance level is user controlled and Cisco has no direct access to this data. If greater security is required, the virtual disks can be encrypted within the environment with the client retaining the keys.

Cisco Cloud Offering	Response
	Data Segregation Each of our clients has their own private cloud, which is physical infrastructure (servers, networking, and storage) within their data center - called an Availability Zone. Each of our clients controls the access to their own availability zones and underlying hardware because it’s in their own data center and the data is segregated and held within each private cloud.
WebEx	If a Host chooses to record a WebEx meeting session, the recording will be stored within the Cisco WebEx Cloud and can be accessed in the My Recordings area on your customized WebEx site. The file will be created only if a Host enables Network Based Recordings (NBR) during the meeting or chooses a site-wide option to record all meetings. NBRs can be accessed through URL links. Each link contains a non-predictable token. The Host has full control of access to an NBR file, including the ability to delete it, share it, or add a password to protect it. The NBR function is optional and can be turned off by the administrator. ■ Access and activities are tracked in audit logs. ■ Cisco WebEx and engaged independent penetration testers audit that access to your recordings cannot be compromised. ■ Recordings are stored in secure zones. All Cisco WebEx Meeting services’ communications are tagged with metadata for multi-tenant isolation. Multiple metadata tags isolate each customer data flow through the system and isolate any customer data-at-rest. The segregation of customer data is logically segmented and, as such, customer data may be produced for a single tenant only. Least privilege job function and role-based access granted to billing and support personnel on customer facing services. Cisco WebEx management reviews WebEx personnel role-based access quarterly and security revokes access if no longer required. Damaged/decommissioned disks are degaussed before removal from data center. Media are certified as erased by e-waste vendor. Global Compliance Enablement (GCE) also performs yearly risk assessments and analyses of functions and countries to determine whether there are any gaps in legal and regulatory compliance and provides guidance in implementing remediation plans. The VP for GCE reports to the Chief Compliance Officer as well as the Audit Committee. Cisco personnel would not in the normal course of business have access to subscriber’s stored data. Cisco further confirms

Cisco Cloud Offering	Response
	that any subscriber stored data or otherwise privileged and confidential information stored in the Cisco WebEx environment and accessible to Cisco WebEx personnel would be controlled by Cisco's WebEx access and password policies and Cisco WebEx credentials.
Spark	Spark is an API based cloud service and it is the intention not to maintain customer data on the cloud. Rather, we use REST API's to grab the customer's data from their data sources, using secure methods, then we complete the call or session. The Customers data will not be held onsite after the call is completed.
Cloud Email Security	Information security, and the protection of database assets and intellectual property, begin with awareness and education. To develop and preserve a culture of security, successful organizations recognize that responsibility and accountability reside with all employees. At Cisco, the executive team has embedded security into corporate initiatives and its code of business conduct, and employees are assimilating security in their daily activities. Employees are educated about the importance of security awareness throughout the organization, and everyone works toward the common goal of keeping the company (and its partners and customers) secure. Human controls are becoming an important aspect of data center security. The aim of these controls is to protect customer data against security threats that may arise from within the service provider. Cisco ROS has a number of controls in place that help ensure customer data security. Cisco conducts background screenings as part of the hiring process for all full-time and contract employees. Job descriptions outline roles and responsibilities within Cisco ROS, and the rule of least privilege is applied to help ensure proper access to customer networks and information. Additional human controls employed by Cisco ROS include: ■ Auditing and testing: Exposure to network-based threats is mitigated through a five-step process. The process requires defining a security policy, assessing compliance, monitoring for policy violations, and routinely testing the policy to reduce exposure. Finally, all identified threats and exposures are reviewed to improve the overall security of the network. ■ Change control: Change control is critical to the operation of any IT environment. Cisco ROS service delivery teams work with customers to establish the proper authorizations for requesting, scheduling,

Cisco Cloud Offering	Response
	implementing, and validating all changes within the customer environment.
Cloud Web Security	Access to private and confidential data on Cisco CWS systems is limited to only those employees with a specific need to retrieve this information. Cisco CWS uses best practice computer security safeguards to protect its databases and servers against risks of loss, unauthorized access, destruction, misuse, modification, or inadvertent or improper disclosure of data. ■ Customer web requests are stored on a separate database and server that can be accessed by only a limited number of Cisco CWS employees. Cisco CWS only accesses data for threat and statistical purposes and only on an anonymous basis. Cisco segregates any personally identifiable information provided by customers. ■ Cisco Cloud Web Security operates a multi-tenant architecture. Customers can access only their own data based on hierarchical access control via ScanCenter with a user-defined password. Customer data is logically separated to prevent any accidental overlap.
Meraki	The Cisco Meraki cloud does not see any actual customer traffic. The Meraki cloud only collects out-of-band management information. The Cisco Meraki cloud is also PCI DSS 3.0 Level 1 and HIPAA certified. Customer data is also protected with 24x7 automated intrusion detection, IP and port-based firewalls, remote access is restricted by IP address and verified by public key (RSA), systems are not accessible via password access, and administrators are automatically alerted on configuration changes. Customers can also block Meraki employees from accessing all of their network management data with a single click in the Meraki dashboard. This block must be temporarily disabled to open a support ticket.
Tropo	Tropo is an API based cloud service and it is the intention not to maintain customer data on the cloud. Rather, we use REST API's to grab the customers' data from their data sources, using secure methods, then we complete the call or session. The Customers data will not be held onsite after the call is completed.
Cisco Energy Management	No user data is accessed by this solution.
Cloud Consumption as a Service	The Cisco Cloud Consumption as a Service cloud does not see any actual customer traffic.

8.6 (E) 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.

Cisco Response:

The Cloud Services offered as part of this proposal 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 received.

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.

Cisco Response:

Table 17. Standards Organization Security Certifications

Cisco Cloud Offering	Response
Metapod	Metapod is a private cloud on customer premises and consequently, the compliance is a shared responsibility with the customer. We are currently finalizing the assessment of the gap for SOC2, PCI, and FISMA and plan to achieve SOC2 compliance. We are also looking at HIPAA and ISO 27001. We are open to consider together with the customer the compliance with standard certifications.
WebEx	Cisco WebEx ISO 27001 Information Security Management Program renewed October 2015.
Spark	ISO 27001, SAS 70,SSAE 16
Cloud Email Security	ISO 27001, SAS 70,SSAE 16
Cloud Web Security	SSAE16 SOC-1 Type II/SOC-2 Type II ISO 27001 ISO 9001 ISO 20000.
Meraki	The Cisco Meraki cloud is PCI DSS 3.0 Level 1, HIPAA, and SAS70 type II/SSAE16 certified.
Tropo	ISO 27001, SAS 70,SSAE 16
Cisco Energy Management	ISO 27001, SAS 70,SSAE 16
Cloud Consumption as a Service	SAS 70,SSAE 16

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.

Cisco Response:

Customer data is protected with 24x7 automated intrusion detection, IP and port-based firewalls, and remote access is restricted by IP address and verified by public key (RSA). Systems are not accessible via password access and administrators are automatically alerted on configuration changes. Customers are not allowed to run any code on Cisco cloud and customer's data is separated using data center best practices.

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).

Cisco Response:

Cisco Data Protection Program

Cisco respects and is committed to protecting our customer's data. We follow privacy policies and data protection practices not only to comply with the law but to earn the trust and confidence in Cisco.

We strive to create the best possible customer experience. Protecting your data is integral to this experience. Everyone at Cisco is responsible for protecting Cisco, our products, our customers, and the customer data that is entrusted to us.

Our Customer Data Protection Program

This established program includes mandatory training for all Global Services employees and new learners at Cisco. Customer Data Protection Training is also an integral part of our COBC annual certification training.

The Customer Data Protection Training focuses on educating global employees to make sure they understand:

- Our customer data protection risk principles
- The importance of their role and the impact they have on the proper handling and protection of customer data
- Customer data protection best practices in their daily roles
- Procedures for reporting an actual or suspected loss of customer data.

Our Code of Business Conduct

All regular Cisco employees are required to complete the Code of Business Conduct (COBC) certification each year. As per the COBC, Cisco employees are required to protect customer data and reduce risk.

Data Security by Design

At Cisco, data security by design means that security is not an add-on but a core component of the development of our products, services, and systems. A dedicated Cisco team provides guidance and targeted training on designing with security in mind throughout our business.

Our Global Compliance Program

Compliance with privacy regulations is managed by representatives from our legal, IT, information security, sales, services, marketing, and human resources teams.

- Training is a key component of our compliance program. We make online privacy training modules and resources available to all employees and contractors through our internal privacy portal. We also provide specific security training relevant to their roles.
- In FY14, Cisco retained the Privacy Seal of TRUSTe, an independent third party whose mission is to foster online trust among consumers and global organizations. This certification demonstrates our commitment to ensuring that our privacy policy and programs meet the industry's best practices for transparency, accountability, and choice in the collection and use of personal information.

Data Protection Assurances You Should Know

- Cisco has an established Customer Data Protection Program focused on building sustainable practices.
- Global employees are trained and certified on Customer Data Protection risk principles and best practices.
- We have internal processes in place to submit, research, and manage data loss incidents.
- The Customer Data Protection Program has executive sponsorship by John N. Stewart, Cisco's Chief Security and Trust Officer and Senior Vice President.
- We are committed to delivering customer data security by design for all products and services.

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.

Cisco Response:

All Cisco offerings are SOC2 audited; several offerings are ISO 27001 certified. Depending on the cloud offering, additional reports and information may be available to assist in customer required certifications such as HIPAA, CJIS, etc. Upon request by an End User Agency, Cisco would support the agency in any security information required to meeting customer-required security certification and processes.

Cisco WebEx is in process of FedRAMP certification Authority to Operate. There is no specific date for the authority to grant operational status.

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.

Cisco Response:

The Computer Security Incident Management Policy specifies the requirements for managing computer security incidents, including but not limited to, detecting, responding, investigating, monitoring, and logging. Failure to comply with this policy may violate privacy law and compromise confidential corporate data, customer data, or employee data. To prevent or minimize such risks, this policy grants the authority for managing computer security incidents and defines the standards for such activities. Cisco does not differentiate logging of activities of remote users from those onsite. Logging and monitoring implementation depends on the systems or services accessed. Unique user IDs allow for a complete trace of user's activities across the systems. VPN session logging provides start-stop information for remote users.

Cisco believes in the value of, and is committed to, the government security certification process. We deliver the right products and services with the right certifications to meet and exceed Public Sector customer expectations. The government certification business is complex. Therefore, Cisco has a dedicated resource team for overall program management of global government certifications and is our third pillar of excellence in support of building and delivering Trust Worthy products and services.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Cisco Response:

Table 18. Visibility of Data

Cisco Cloud Offering	Response
Metapod	As part of our managed solution, we deal with all the log data through our virtual NOC and will alert the customer if any threshold has been exceeded. There are a few different tools we use to generate log data so that we can have good picture as to the health of the environment. We would also be open to explore what types of log data the customer requires as it has been requested by other clients and we want to understand requirements before we put it on our product roadmap. Service levels are monitored by analyzing various logging collection points: Bare metal statistics, Host OS logs, infrastructure logs, and OpenStack logs.
WebEx	The WebEx recording link can only be created/password protected by the host and disseminated to attendees. Attendees must authenticate to view/hear recording. Recording content is tagged for voice, audio, and metadata steams and the streams are stored on separate servers and are meaningless in isolation.
Spark	Since SPARK has the basic functions of a call to deliver its service all calls have a Call Detail Record associated with each

Cisco Cloud Offering	Response
	call.
Cloud Email Security	The Customer will be provided access by Cisco to a web-based interface to administer and report on the Services. Access to the interface is via a secure (HTTPS) website and is password-protected. The Customer may have multiple administrators for a single account. The Customer can request a unique login for each administrator and provide full access or read only privileges specific to each user. The interface enables the customer administrator to: ■ Review statistics of all malware stopped and other email content blocked ■ Create access restrictions and apply these to specific users or groups ■ Configure and schedule automated system reporting ■ Track email messages. Customers also can access a comprehensive support portal with an extensive knowledge base of subject matter expertise to assist with their needs. Using this support portal, customers can view all current and historical events/tickets, reports, as well as the status of their cloud service infrastructure.
Cloud Web Security	Access to private and confidential data on Cisco CWS systems is limited to only those employees with a specific need to retrieve this information. Cisco CWS uses best practice computer security safeguards to protect its databases and servers against risks of loss, unauthorized access, destruction, misuse, modification, or inadvertent or improper disclosure of data. ■ Customer web requests are stored on a separate database and server that can be accessed by only a limited number of Cisco CWS employees. Cisco CWS only accesses data for threat and statistical purposes and only on an anonymized basis. Cisco segregates any personally identifiable information provided by customers. ■ Cisco Cloud Web Security operates a multi-tenant architecture. Customers can access only their own data based on hierarchical access control via ScanCenter with a user-defined password. Customer data is logically separated to prevent any accidental overlap.
Meraki	The Cisco Meraki cloud supports role-based access control to restrict the data available to specific users or groups.
Tropo	Since Tropo has the basic functions of a call to deliver its service all calls have a Call Detail Record associated with each

Cisco Cloud Offering	Response
	call.
Cisco Energy Management	Not Applicable
Cloud Consumption as a Service	Not Applicable

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.

Cisco Response:

Purchasing Entity identified contact will be notified in 48 hours of a confirmed breach by the Incident Commander in writing or as specified in the contract. The Data Protection and Privacy team within Cisco's Security and Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging the talents of diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

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.

Cisco Response:

Cisco has an in-depth defense strategy to maintain system integrity, which includes restrictive ACLs that block common ports between differing security zones. Cisco uses multiple active host management technologies to identify vulnerabilities and mitigate risks.

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).

Cisco Response:

Table 19. Security Technical Reference Architectures

Cisco Cloud Offering	Response
Metapod	Since the on-prem cloud is deployed within a client's IT framework, all of their security practices would apply from a network and external firewall perspective. We also provide tools to place firewall rules on VMs within the cloud through OpenStack security groups, for another layer of security. Cisco Systems can also work with the customer to architect the best solution to meet any intrusion detection and/or prevention demands. We have hardware and software based intrusion detection and prevention apparatus plus managed service offerings from Sourcefire, a Cisco entity. We will work with the customer to architect the best and most accommodating solution

Cisco Cloud Offering	Response
	to address the need and its management challenges.
WebEx	Cisco WebEx Cloud Collaboration deploys a globally distributed dedicated network of high-speed meeting switches. Meeting session data originating from the presenter's computer and arriving at the attendees' computers is switched, never persistently stored, through the Cisco WebEx Cloud unless the host records the meeting. The web server, application, telephony, and data base servers are physically separate. Web server manages communication requests and provides meeting site host information and client session. The application server provides the active and standby meeting session. The telephony server provides conference bridging through VOIP. WebEx meeting attendees connect to the Cisco WebEx Cloud using a logical connection at the application/presentation/session layers. There is no peer-to-peer connection between attendees' computers. Cisco WebEx does not release its proprietary detailed architecture diagrams.
Spark	This is a new offer and this information is proprietary and not available at this time.
Cloud Email Security	CES and CWS are operated as services and deployed using Cisco best practices for Data Center architectures. There are no service elements available that can be deployed except as protocol layer service elements (SMTP and HTTP/S and FTP over HTTP) and the apparatus to support these services is self-contained.
Cloud Web Security	CES and CWS are operated as services and deployed using Cisco best practices for Data Center architectures. There are no service elements available that can be deployed except as protocol layer service elements (SMTP and HTTP/S and FTP over HTTP) and the apparatus to support these services is self-contained.
Meraki	The Meraki cloud does not support IaaS or PaaS. Security best practices for Cisco Meraki accounts are documented at https://meraki.cisco.com/trust#tools.
Tropo	This is a new offer and this information is proprietary and not available at this time.
Cisco Energy Management	Not Applicable
Cloud Consumption as a Service	Not Applicable

8.7 (E) 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.

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.

Cisco Response:

Table 20. Return of Data

Cisco Cloud Offering	*Response*
Metapod	**Surviving Software License**. a. **Proprietary Software License**. Upon expiration or termination of the applicable SOW, payment of all fees that are due and owing, and subject to payment for the Services, and the terms and conditions of the SOW and this Agreement, Cisco grants Customer a worldwide, limited, non-exclusive, non-sub licensable, perpetual, non-transferable right to use Software as installed on Cisco or Customer owned or leased hardware **on Customer's premises** or data centers owned or otherwise controlled by Customer. b. **Open-Source Software License**. Upon termination or expiration of the applicable SOW, Customer can use, copy, redistribute, or modify the Open Source Software under the terms and conditions of the corresponding Open Source Software licenses in effect at that time. If required by the applicable Open Source Software license, Customer may obtain a copy of, or access to the source code corresponding to the binaries for the open source software used in the Software from Cisco upon request. Customer agrees to comply with the applicable licenses and additional terms and notices for such Open Source Software. Cisco makes no warranties or representations of any kind to Customer regarding the performance of the Open Source Software. Upon expiration or termination of the applicable SOW, Customer will not be entitled to any services with respect to such use of the Software unless subject to a separate written agreement with Cisco. Cisco Metapod is an on-premises deployment, on customer hardware. Upon the termination of the contract, all data remains in place.
WebEx	Cisco WebEx will retain subscriber for a reasonable period of time after notice of termination. Recordings will be returned in electronic format (.WRF) to the point of contact.

Cisco Cloud Offering	Response
Spark	Data can be securely exported. If the Subscriber terminates the Service for convenience (as allowed under the Spark Terms of Service, and effective upon expiration or termination of all outstanding Orders), the organization's Business Messaging account will be converted to the entry level, no-cost Business Messaging offer ("Free Spark"). The Storage included with Free Spark will be 5GB per User, but may not be pooled amongst Users. Additional terms applicable to Free Spark are set forth in the Spark Terms of Service.
Cloud Email Security	CWS and CES Customer accounts and service settings can be migrated within the service themselves and are managed and migrated to Cisco owned and operated infrastructure alternative servers and data centers at the discretion of Cisco. External customer interaction and management of service policy in the services are not impacted.
Cloud Web Security	CWS and CES Customer accounts and service settings can be migrated within the service themselves and are managed and migrated to Cisco owned and operated infrastructure alternative servers and data centers at the discretion of Cisco. External customer interaction and management of service policy in the services are not impacted.
Meraki	If a customer decides to end their Cisco Meraki deployment, they should power down all Meraki on- premise hardware. This will halt the flow of new information into the Meraki cloud. Network management data currently in the Meraki cloud can be securely exported.
Tropo	Not Applicable
Cisco Energy Management	Data can be securely exported. Customer understands and acknowledges that it is solely and fully responsible for backing-up and/or otherwise protecting its own data against loss, damage, or destruction.
Cloud Consumption as a Service	Not Applicable

8.8 (E) 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.
b. Suffers an unrecoverable loss of data.
c. Offeror experiences a system failure.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Cisco Response:

Cisco's Service Level Agreement relates specifically to the uptime of the Cisco solution. Our solution has been designed to tolerate hardware failures for our controller tier and our hypervisor tier and it is assumed there will be network availability for this project that is outside the scope of this project. [Client] may request support by opening a ticket via Cisco's support website, email or by calling Cisco support. An "incident" begins when Cisco's operations team determines that intervention is required, when monitoring software detects an issue or when the Client notifies Cisco either by phone or by e-communication. SLAs for incident response are detailed in Table 21 below:

Table 21. Service Or Data Recovery

Cisco Cloud Offering	Response
Metapod	The Standard Operating Procedures for an outage are: ■ Cisco receives notification of an outage through either an automated message, our own personnel, or the customer ■ A Cisco Advanced Services team member is assigned as point on the issue ■ An audio/video bridge is established to link Cisco Advanced Services personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ■ Email to client mailing list and escalation person(s) via Support Ticketing System ■ Alternate means of contact to escalation person(s) as specified by playbook contact method ■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent ■ Customer conference call is scheduled to discuss the outage ■ Report is made available to customer within a set time after an outage. Cisco will use commercially reasonable efforts to make the Cisco Metapod Platform, comprising of the Control Plane and the Data Plane, available with a Monthly Uptime Percentage of at least 99.99 percent, in each case during any calendar month during the End User subscription term ("Service Commitment"). In the event that the Control Plane or Data Plane does not meet the Service Commitment, End User will be eligible to request a Service Credit as described below. **Definitions** "Control Plane" means the applications that provide the cloud

Cisco Cloud Offering	Response
	Application Programming Interfaces (APIs) and website interfaces used to manage cloud resources in an Availability Zone. “Data Plane” means the network that is used to connect the Control Plane to the servers that run virtual instances. “Monthly Uptime Percentage” is calculated by subtracting from 100 percent the percentage of minutes during the calendar month in which the Control Plane or Data Plane in a single Availability Zone, as applicable, was in the state of “Unavailable.” Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Cisco Metapod Service Level Agreement Exclusions (defined below). “Unavailable” or “Unavailability” means: ■ For Control Plane, when all requests to facilitate consumption of cloud resources, via the API or website interfaces, are unable to be accessed because they are down or unresponsive to requests. ■ For Data Plane, when all End User running instances have no external connectivity. A “Service Credit” is the number of days, as calculated below, that Cisco may add to the end of End User subscription term. Cisco Metapod covers the IaaS layer data protection and recovery for on-prem clouds are typically performed by our clients; Customer owns the VM instances as well as the application data and have the most knowledge of the needs. Most of our customers use a higher level orchestration system either built in house or using standard tool sets (e.g., Chef, Puppet, Ansible, Cloud Foundry, RightScale, Cliqr) to build or redeploy a DR landing zone should a disaster occur. This is generally tied into the application as well, where it can perform auto healing based on the types of behavior it sees in the infrastructure. If, however, a further disaster recovery is necessary, the broader Cisco organization can absolutely help the customer develop a five nines DR apparatus using hardware based load balancers, balancing across physically disparate availability zones to software based load balancers controlling the web, app, and DB tiers. This would be based on the customer architecture requirements and can be handled as part of the broader cloud solution. As described above; Metapod covers the IaaS layer and not the guest OS and user application layer. For on-prem clouds, data protection and recovery are typically performed by our clients; they own the VM instances as well as the application data and have the most knowledge of the needs. Most of our customers use a higher level orchestration system either built in house or

Cisco Cloud Offering	Response
	using standard tool sets (e.g., Chef, Puppet, Ansible, Cloud Foundry, RightScale, Cliqr) to build or redeploy a DR landing zone should a disaster occur. This is generally tied into the application as well, where it can perform auto healing based on the types of behavior it sees in the infrastructure. If, however, a further disaster recovery is necessary, the broader Cisco organization can absolutely help the customer develop a five nines DR apparatus using hardware based load balancers, balancing across physically disparate availability zones to software based load balancers controlling the web, app, and DB tiers. This would be based on the customer architecture requirements and can be handled as part of the broader cloud solution. Cisco's Service Level Agreement relates specifically to the uptime of the Cisco Metapod solution. Our solution has been designed to tolerate hardware failures for our controller tier and our hypervisor tier and it is assumed there will be network availability for this project that is outside the scope of this project. The client may request support by opening a ticket via Cisco's support website, email, or by calling Cisco support. An "incident" begins when Cisco's operations team determines that intervention is required, when monitoring software detects an issue or when the Client notifies Cisco either by phone or by e-communication. SLAs for incident response are detailed below: Severity — Initial Response — Time To Recovery Plan Emergency — Immediate (< 1 hour) — Within 4 hours Urgent — 8 hours — Within 12 hours Standard — 24 hour — Within 48 hours
WebEx	Services are not affected because a redundant, alternate meeting site operates in active mode in the background. Cisco WebEx Global Site Backup (GSB) Tier-1 clusters replicate production data continuously throughout the day and will automatically be used as a failover site should the primary site become unusable or the core meeting service be temporarily disrupted. Tier-2 storage devices hold backups of Tier-1 storage and are stored on separate storage servers from Tier-1 storage. As part of disaster recovery procedures, Tier-2 storage is replicated bi-directionally across geographically separated Cisco WebEx data centers to ensure that data is stored in more than one data center. Cisco would recover mission-critical and business functions based on its requirements for infrastructure recovery. RTO is dependent on nature/severity of incident.
Spark	Tropo/SPARK is fully redundant cloud model with recoverable data. The only data that sits in the cloud is the program API's that are created by the developers and fulfil the actions that are

Cisco Cloud Offering	Response
	dictated by the program. If a full outage happens then Tropo will be able to restore the program or the customer can have a full backup of the last program and will be able to restore upon restoration of the cloud service.
Cloud Email Security	The Standard Operating Procedures for an outage are: ■ Cisco receives notification of an outage through either an automated message, our own personnel, or the customer ■ A Cisco Advanced Services team member is assigned as point on the issue ■ An audio/video bridge is established to link Cisco Advanced Services personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ■ Email to client mailing list and escalation person(s) via Support Ticketing System ■ Alternate means of contact to escalation person(s) as specified by playbook contact method ■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent. ■ Customer conference call is scheduled to discuss the outage ■ Report is made available to customer within a set time after an outage. ■ RTO is not applicable to a SaaS offering.
Cloud Web Security	The Standard Operating Procedures for an outage are: ■ Cisco receives notification of an outage through either an automated message, our own personnel, or the customer ■ A Cisco Advanced Services team member is assigned as point on the issue ■ An audio/video bridge is established to link Cisco Advanced Services personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ■ Email to client mailing list and escalation person(s) via Support Ticketing System ■ Alternate means of contact to escalation person(s) as specified by playbook contact method

Cisco Cloud Offering	Response
	■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent. ■ Customer conference call is scheduled to discuss the outage ■ Report is made available to customer within a set time after an outage. ■ RTO is not applicable to a SaaS offering.
Meraki	Cisco Meraki products remain functional in the event the cloud goes down. Customer's networks will remain operational in the event of a cloud outage. Therefore, extended downtime will not affect customer networks.
Tropo	Tropo/SPARK is fully redundant cloud model with recoverable data. The only data that sits in the cloud is the program API's that are created by the developers and fulfil the actions that are dictated by the program. If a full outage happens then Tropo will be able to restore the program or the customer can have a full backup of the last program and will be able to restore upon restoration of the cloud service.
Cisco Energy Management	The Standard Operating Procedures for an outage are: ■ Cisco receives notification of an outage through either an automated message, our own personnel, or the customer ■ A Cisco Advanced Services team member is assigned as point on the issue ■ An audio/video bridge is established to link Cisco Advanced Services personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ■ Email to client mailing list and escalation person(s) via Support Ticketing System ■ Alternate means of contact to escalation person(s) as specified by playbook contact method ■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent. ■ Customer conference call is scheduled to discuss the outage. ■ Report is made available to customer within a set time after an outage.

Cisco Cloud Offering	Response
	■ RTO is not applicable to a SaaS offering.
Cloud Consumption as a Service	The Standard Operating Procedures for an outage are: ■ Cisco receives notification of an outage through either an automated message, our own personnel, or the customer ■ A Cisco Advanced Services team member is assigned as point on the issue ■ An audio/video bridge is established to link Cisco Advanced Services personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ■ Email to client mailing list and escalation person(s) via Support Ticketing System ■ Alternate means of contact to escalation person(s) as specified by playbook contact method ■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent. ■ Customer conference call is scheduled to discuss the outage ■ Report is made available to customer within a set time after an outage ■ RTO is not applicable to a SaaS offering.

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States.

Cisco Response:

Table 22. Backup and Restore Services Methodology

Cisco Cloud Offering	Response
Metapod	Metapod covers IaaS layer only. While we designed our CEPH and/or Object storage system to be highly distributed (across all VM nodes) it is up to our clients to back up their data and virtual machines. Our platform does provide a way to do a “backup” or “snapshot” of a VM and save it back to the image catalogue. We generally suggest the catalogue be on a persistent storage device such as Ceph pool or an NFS device so that it is protected.

Cisco Cloud Offering	Response
	Users can easily perform a server image back up into Metapod (using OpenStack Glance image management system and CEPH or SWIFT storage components). These operations are available via API, Dashboard, or CLI. The location would be the Object Storage Nodes that are part of Metapod (in case users/admins decide to back up on Object storage) or the CEPH nodes (also part of the Metapod system) in case the users or admins decide to back up on block storage. The alternate location can be either another Cisco Metapod availability zone, in a different location (with either CEPH or Swift Object storage) or an external storage service like Iron Mountain or Amazon S3.
WebEx	The last successful replicated snapshot at both data centers is utilized for backup. Replication to primary and alternate data centers. WebEx recording snapshots put on secondary storage at each data center. Cisco WebEx owned data centers Richardson, TX, Mountain View, CA
Spark	This is not applicable for a SaaS offering and considered proprietary to Cisco.
Cloud Email Security	This is not applicable for a SaaS offering and considered proprietary to Cisco.
Cloud Web Security	This is not applicable for a SaaS offering and considered proprietary to Cisco.
Meraki	Customer’s data is backed up across three distributed data centers. If a customer is, nonetheless, concerned about an unrecoverable loss of data, they can gather exported data from the Meraki cloud for on premise storage. In the event of a severe data center outage, customers automatically failover to a redundant data center that is kept up-to-date in real time. Data is backed up between two data centers in real time with nightly backups to a tertiary location. Backups are securely transported over the Internet to an off-site location. All customer data can be kept in the continental U.S. if requested.
Tropo	This is not applicable for a SaaS offering and considered proprietary to Cisco.
Cisco Energy Management	This is not applicable for a SaaS offering and considered proprietary to Cisco.
Cloud Consumption as a Service	This is not applicable for a SaaS offering and considered proprietary to Cisco.

8.9 (E) 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.

Cisco Response:

Table 23. Data Protection

Cisco Cloud Offering	Response
Metapod	Client data is generally stored within the guest operating system instance, which is owned and managed by the client, on client premises. The security set at the instance level is user controlled and Cisco has no direct access to this data. If greater security is required, the virtual disks can be encrypted within the environment with the client retaining the keys.
WebEx	Cisco WebEx uses AES 128 bit minimum encryption asymmetric cryptography is used for the in transit meeting session communication. sRTP is used to encrypt file sharing in the session. WebEx session certificate authenticity uses RSA 2048 algorithm symmetric cryptography. Passwords are salted and hashed. The Cisco Minimum Encryption Standard follows the Cisco Secure Development Lifecycle Product Security Baseline (PSB) crypto guideline (EDCS-1385142) which outlines (among many other things) acceptable hash, encryption, signature and random number generation functions, SSL/TLS cipher suites, as well as their order of preference.
Spark	The Cisco Spark app uses end-to-end encryption with state-of-the-art cryptographic algorithms. Plus, only people who have successfully authenticated with our service can view messages and files in Cisco Spark rooms. Unauthorized people who try accessing the URL of a room can't see what has been shared. The Cisco Spark app encrypts messages, files, and room names on your device before sending them to the cloud. Content arrives at our servers already encrypted. It's processed (data in use) and stored (data at rest) until it gets decrypted on the intended recipients' devices. We use Secure HTTP (HTTPS) to encrypt data in transit between your device and our servers, which protects the identities of the senders and receivers of the encrypted content. For real-time media (voice, video, and screen sharing), we encrypt what is shared using the Secure Real-Time Transport Protocol (SRTP).
Cloud Email Security	CES uses dedicated portal and email processing infrastructure per customer.
Cloud Web Security	CWS uses a customer specific portal for administrative access.

Cisco Cloud Offering	Response
	Customer access to the portal for management, reporting, and technical support is encrypted and supported on industry standard web browsers. Customer traffic for web security authentication and access to the service is encrypted.
Meraki	All sensitive data in the Cisco Meraki cloud is encrypted.
Tropo	The Cisco Tropo app uses end-to-end encryption with state-of-the-art cryptographic algorithms.
Cisco Energy Management	All data transferred is securely encrypted.
Cloud Consumption as a Service	Not applicable, Customer shall ensure that Data Collection Tool or scripts are located in a secure area, within a Network environment protected within a firewall and on a secure LAN, under lock and key and with access restricted to those Customer employee(s) or contractor(s) who have a need to access the Data Collection Tool and/or a need to know the contents of the output of Data Collection Tool.

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.

Cisco Response:

If appropriate, Cisco is willing to negotiate a Business Associate Agreement with Purchasing Entities.

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.

Cisco Response:

Cisco may aggregate data at a summary level for reporting statistics only. Cisco will not market data and will not use it other than for its intended purpose per the Cisco SaaS Agreement.

8.10 (E) 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.

Cisco Response:

In order to make our offerings available globally, we standardize our Service Level Agreements. Therefore, it is generally not negotiable. With standardized offerings, tools and processes are automated so that they are consistent, replicable and scalable for our customers. With any customized Service Level Agreement, there will be cost impacts to Cisco and the Purchasing Entity. However, Cisco is always open to listening to our customers' concerns, especially if such concerns are related to performance and criteria associated with Cisco's applicable Service Level Agreements.

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. .

Cisco Response:

A sample of the WebEx SLAs can be found below:

- **Availability Level**. WebEx will maintain 99.5 percent availability of its Web Based Application Services (including telephony services) to the Internet (excluding scheduled maintenance intervals) ("Availability Level").
- **Down Time Credit**. For any cumulative time periods in excess of that contemplated by Availability Level for which the Services are unexpectedly unavailable to the Internet ("Down Time"), WebEx or Cisco (in either case, the "Company") will credit the customer (if the purchase is made directly) or reseller (if the purchase is made indirectly) the amount of Subscription Service Fees or License Fees, as applicable, owed in an amount equal to that portion of the month attributable to the Down Time; provided that (i) use of the Services is impacted, (ii) the Down Time is reported within 24 hours of each occurrence, and (iii) the party purchasing from the Company, as applicable, requests credits not more than 30 days after each occurrence. The terms and conditions of this section shall be the purchaser's sole and exclusive remedy and the Company's sole obligation for any Down Time.
- **Confidentiality**. All parties agree that the existence and terms of this SLA and the issuance of any credits in accordance with this SLA, are strictly confidential and shall only be disclosed to the customer or reseller, and to employees of the parties on a "need to know" basis for purposes of fulfilling the parties' obligations hereunder. Neither party will disclose to any third party (other than a purchasing customer) the existence, intent, or terms of this SLA without the prior written consent of the other party.
- **Credit Availability**. If Services are prepaid, a Credit Memo will be issued. The Credit Memos described above may be applied by the party purchasing from the Company toward the purchase of Company products or services (for any end-customer) during the 12 months following issuance of such credits. Any credit not used within such 12 month period shall be void and have no value. Credits may not be converted to refunds, used as set off from any amount owing to Cisco or WebEx, nor transferred or assigned.

Additional SLAs and Service Descriptions can be found in Attachment 3 Service Descriptions and SLAs.pdf.

8.11 (E) DATA DISPOSAL

Specify your data disposal procedures and policies and destruction confirmation process.

Cisco Response:

Table 24. Data Disposal

Cisco Cloud Offering	Response
Metapod	In Cisco Metapod solution, user data resides on customer premises (Metapod Ceph and Swift storage is distributed across hard drives (SAS/SSD) in the VM servers).
WebEx	A remedy ticket must be submitted to and approved by the Data Center Operations Manager before the data center asset can be disposed. Hard drives are degaussed. A certificate of disposal is provided by an e-waste vendor ensuring all hardware was destroyed.
Spark	All programs created with customer's accounts whereas not containing data but the code to retrieve and execute the program will be lost once the account is deleted.
Cloud Email Security	Cisco CEM supports secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the end user.
Cloud Web Security	Cisco CEM supports secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the end user.
Meraki	Only network management data resides in the Cisco Meraki cloud. All network management data eventually is deleted from the Meraki cloud. The timeframe for deletion depends on the type of data.
Tropo	All programs created with customers' accounts whereas not containing data but the code to retrieve and execute the program will be lost once the account is deleted.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.12 (E) 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.

Cisco Response:

Table 25. Performance Measures And Reporting

Cisco Cloud Offering	Response
Metapod	Cisco Metapod offers a 99.99 percent service availability. Cisco has a clear advantage in Private Cloud Management Services because of several years of production engineering developing

Cisco Cloud Offering	Response
	the tools and automation required for large scale and detailed proactive monitoring. Our Fortune 100 customers demand it. Over 50 different bare metal performance data collection points as well as capacity monitoring, trending, and reporting mean that the Advanced Support team is always providing responsive service. In order to prevent an outage, we have designed our solution with redundant control points (n+2) ensure that OpenStack orchestration services remain available even if a node fails. The cloud software will be configured using a High Availability (HA) model. HA is achieved by configuring the system to use a refined combination of mature and proven open-source techniques and technologies like Clustering, Quarum, Corosync, Pacemaker, and HA Proxy, to name a few. The system architecture has been designed so that there is no single point of failure.
WebEx	WebEx will maintain 99.5 percent availability of its Web Based Application Services (including telephony services) to the Internet (excluding scheduled maintenance intervals) (Availability Level).
Spark	Tropo/SPARK offers 99.99 percent availability SLA
Cloud Email Security	Cisco's Email Security SLA is Actual Uptime < 99.999 percent.
Cloud Web Security	Cisco's Cloud Web Security SLA is 99.5 percent.
Meraki	Cisco Meraki’s cloud infrastructure is covered under a 99.99 percent SLA and the Cisco Meraki Infrastructure team manages it 24×7×365 to ensure high availability.
Tropo	Tropo/SPARK offers 99.99 percent availability SLA
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

Cisco Response:

Table 26. Standard Uptime SLA Criteria

Cisco Cloud Offering	Response
Metapod	**Service Commitment** Cisco will use commercially reasonable efforts to make the Cisco OpenStack Private Cloud Platform, comprised of the Control Plane and the Data Plane, available with a Monthly Uptime Percentage (defined below) of at least 99.99 percent, in

Cisco Cloud Offering	Response
	each case during any calendar month during the End User subscription term (Service Commitment). In the event that the Control Plane or Data Plane does not meet the Service Commitment, End User will be eligible to request a Service Credit as described below. **Definitions** “Control Plane” means the applications that provide the cloud Application Programming interfaces (APIs) and website interfaces used to manage cloud resources in an Availability Zone. “Data Plane” means the network that is used to connect the Control Plane to the servers that run virtual instances. “Monthly Uptime Percentage” is calculated by subtracting from 100 percent the percentage of minutes during the calendar month in which the Control Plane or Data Plane in a single Availability Zone, as applicable, was in the state of “Unavailable.” Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Cisco Metapod Service Level Agreement Exclusions (defined below). “Unavailable” or “Unavailability” means: ■ For Control Plane, when all requests to facilitate consumption of cloud resources, via the API or website interfaces, are unable to be accessed because they are down or unresponsive to requests. ■ For Data Plane, when all End User running instances have no external connectivity. A “Service Credit” is the number of days, as calculated below, that Cisco may add to the end of End User Subscription Term. **Service Commitment and Credits** Service Credits are calculated as the number of days that Cisco may add to the end of the Term at no charge to End User for either a Control Plane or Data Plane outage (whichever was Unavailable) in the Availability Zone affected for the calendar month in which the Unavailability occurred in accordance to the schedule below. If both the Control Plane and Data Plane were Unavailable, the lower of the Monthly Uptime Percentage will determine the Service Credit applied. End User must notify Cisco of any Unavailability for which End User is claiming Service Credits, including the following: ■ Services impacted and claimed Service Level failure ■ Any activities performed prior to the claimed Service Level failure ■ Business impact of service outage/disruption.

Cisco Cloud Offering	Response
	Any other reasonably requested information pertaining to the claimed Service Level failure (i.e., support ticket #). Cisco will determine whether a Service Credit is due in its sole discretion. **Monthly Uptime Percentage** Less than 99.99 percent but equal to or greater than 99.9 percent Less than 99.9 percent but equal to or greater than 99.0 percent Less than 99.0 percent **Service Credit** 3 days 7 days 15 days Cisco will begin measuring the Monthly Uptime Percentage 1 calendar month after the Availability Zone has been setup and End User has access to the environment. This period of time allows End User and Cisco to evaluate the Services are being performed as specified and the platform is operating according to the Documentation. **Cisco Metapod Service Level Agreement Exclusions** The Service Commitment does not apply to any services that expressly exclude this Service Commitment (as stated in the documentation for such services) or any unavailability, suspension, or termination of Cisco Metapod performance issues: (i) that result from End User breach of the Cisco Metapod Service or the Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Cisco Metapod; (iii) that result from any actions or inactions of End User or any third party; (iv) that result from End User equipment, software, or other technology and/or third-party equipment, software, or other technology (other than third-party equipment within Cisco's direct control); (v) that result from failures of individual instances or individual servers not attributable Unavailability; (vi) that result from any maintenance as provided for pursuant to the Cisco Metapod Agreement, or (vii) where End User fails to maintain controller equipment under a valid device level Cisco Technical Services contract with at least 8x5xNBD coverage. If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion. **Maintenance Terms** From time to time, we may apply upgrades, patches, bug fixes, or other maintenance to the Service Offerings (Maintenance). We agree to use reasonable efforts to provide End User with 72 hours prior notice of any scheduled Maintenance (except for

Cisco Cloud Offering	Response
	emergency Maintenance) and End User agrees to use reasonable efforts to comply with any Maintenance requirements for which we notify End User.
WebEx	WebEx will maintain 99.5 percent availability of its Web Based Application Services (including telephony services) to the Internet (excluding scheduled maintenance intervals) (Availability Level).
Spark	Standard uptime is 99.99%
Cloud Email Security	The Cloud Email Security Service will accept connections on Port 25 and process email at least 99.999 percent over a trailing 1-year period. Uptime is determined by dividing the total number of minutes the Service was processing email divided by the number of minutes in a 1-year period or 525,600 minutes. Downtime must exceed 30 seconds per occurrence before it is an infraction. An infraction is limited to a single incident, whereby separate downtime occurrences cannot be aggregated. Uptime is determined and validated by an industry-recognized third-party monitoring service that performs service-level checks from various locations on the global Internet.
Cloud Web Security	Cisco warrants that its network will process and deliver Customer’s web requests at least 99.999 percent of the total hours during every month Customer uses the Service (Availability). Availability will be determined on an aggregate basis across all Customer sites. Cisco provides both primary and secondary proxy addresses for each site from which web traffic may be directed. As a result, non-Availability occurs only where web content sent from a site to both proxy addresses is not being received or transmitted to end users at the affected Customer site.
Meraki	During the Term, the Hosted Software will be operational and available to Customer at least 99.99% of the time in any calendar month. The complete Meraki SLA is available in Attachment 3.
Tropo	Standard uptime is 99.99%
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

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.

Cisco Response:

Cisco will make available Cisco's support available 24 hours per day, 7 days per week to assist by telephone, fax, electronic mail, or the Internet. Cisco will respond within one (1) hour for all calls received during Standard Business Hours and for Severity 1 and 2 Incidents and 2 hours for Severity 1 and 2 calls received outside Standard Business Hours. For Severity 3 and 4 calls received, Cisco will respond no later than the next Business Day.

Cisco will manage Incidents and Problems according to the Cisco Severity and Escalation Guideline, as modified below.

Cisco will provide Customer with access to Cisco.com. This system provides Customer with helpful technical and general information on Cisco products as well as access to Cisco's on-line Software Center library. Please note that access restrictions identified by Cisco from time to time may apply.

Cisco will have no responsibility for providing support for third party software or hardware.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Cisco Response:

The SLA remedies available to the customers will vary by each Cisco offering. However, below are some examples of the remedies available:

Table 27. SLA Remedies

Cisco Cloud Offering	*Response*
Metapod	Service Credits are calculated as the number of days that Cisco may add to the end of the Term at no charge to End User for either a Control Plane or Data Plane outage (whichever was Unavailable) in the Availability Zone affected for the calendar month in which the Unavailability occurred in accordance to the schedule below. If both the Control Plane and Data Plane were Unavailable, the lower of the Monthly Uptime Percentage will determine the Service Credit applied. End User must notify Cisco of any Unavailability for which End User is claiming Service Credits, including the following: ■ Services impacted and claimed Service Level failure ■ Any activities performed prior to the claimed Service Level failure ■ Business impact of service outage/disruption ■ Any other reasonably requested information pertaining to the claimed Service Level failure (i.e., support ticket #). Monthly Uptime Percentage — Service Credit ■ Less than 99.99 percent but equal to or greater than 99.9 percent — 3 days

Cisco Cloud Offering	Response
	■ Less than 99.9 percent but equal to or greater than 99.0 percent — 7 days ■ Less than 99.0 percent — 15 days. Cisco will begin measuring the Monthly Uptime Percentage 1 calendar month after the Availability Zone has been setup and End User has access to the environment. This period of time allows End User and Cisco to evaluate the Services are being performed as specified and the platform is operating according to the Documentation.
Cloud Email Security	If Customer experiences a downtime infraction and subject to the General Exceptions (as defined below), then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy: Mailbox Count: 250+ 2,000+ 5,000+ 10,000+ 20,000+ Actual Uptime < 99.999 percent $100 $200 $500 $1,000 $2,000 Customer may only make a total of two claims of a downtime occurrence within a rolling 365-day period. If Customer experiences three or more downtime occurrences within a rolling 365 day period, IronPort and Customer will come to a written agreement, within 30 days of Customer providing notice of such occurrence, on the next course of action. If Customer experiences a downtime infraction more than five within a rolling 365-day period and IronPort fails to provide a reasonable written plan of permanent corrective action to customer within a 30-day time frame after the fifth occurrence, then Customer shall have the right to cancel the Services at no cost or obligation and no financial responsibility for any future payments. Customer responsibilities: ■ Customer must provide notice within 30 days of the downtime occurrence ■ Customer must provide timeframe details of the downtime occurrence, any correlated support ticket numbers, and, if available, pings and trace routes showing that the device was not available on the network ■ Customer must provide confirmation, if possible, that there were: ❑ No network failures at the customer site either internal or external at the time of the occurrence ❑ No Customer implemented changes that adversely affected the system availability or made the system to cause delays (excepting any changes requested by IronPort)

Cisco Cloud Offering	Response
	❑ No material delay in responding to warnings raised by IronPort generally, or specifically related to the incidence of downtime.
Cloud Web Security	If Cisco breaches the Availability warranty, Cisco shall provide service credits of a portion of Customer’s monthly Service fees on the following basis: Monthly Service Availability percent reimbursement of monthly Service fee: ■ 99.999 — 99.5 percent 10 ■ 99.49 — 99.0 percent 20 ■ 98.99 — 98.5 percent 30 ■ 98.49 — 98.0 percent 40 ■ 97.99 — 97.5 percent 50 ■ 97.49 — 97.0 percent 60 ■ 96.99 — 96.5 percent 70 ■ 96.49 — 96.0 percent 80 ■ 95.99 — 95.5 percent 90 ■ Below 95.5 percent 100.
Meraki	Service Level Warranty. During the Term, the Hosted Software will be operational and available to Customer at least 99.99 percent of the time in any calendar month (the Service Level Warranty). If the Monthly Uptime Percentage does not meet the Service Level Warranty in any calendar month, and if Customer meets its obligations under this Agreement, then Customer will be eligible to receive Service Credit as follows: < 99.99 percent — ≥ 99.9 percent 3 Days, < 99.9 percent — ≥ 99.0 percent 7 days, < 99.0 percent 15 days.

8.12.5 Intentionally Deleted.

8.12.6 Describe the firm’s procedures and schedules for any planned downtime.

Cisco Response:

Table 28. Planned Downtime

Cisco Cloud Offering	Response
Metapod	Some of the aspects that are out of the control of Metapod include but are not limited to, interruptions failures or delays to customer network access or connections, third-party Internet service provider interruptions failures or delays, or any defect or failure in any hardware or servers provided by the customer. Metapod offers a 7x24x365 monitoring and support model as part of this offer with the Standard Operating Procedures for an outage being:

Cisco Cloud Offering	Response
	■ Automated alerting, Metapod personnel, or Customer initiated notification of outage is received ■ Metacloud Advanced Services team member assigned as point on the issue ■ Audio/video bridge established to link Metapod personnel assigned to the event ■ Investigation and drive to rapid resolution is undertaken ■ Customer-facing communications, tickets, and escalations are initiated ❑ Email to client mailing list and escalation person(s) via Support Ticketing System ❑ Alternate means of contact to escalation person(s) as specified by playbook contact method ■ If outage continues, updates to customers continue at set intervals ■ At the conclusion of an outage, a summary wrap up message is sent ■ Customer conference call is scheduled to discuss the outage ■ Report is made available to customer within a set time after an outage. Metapod solution has been designed to tolerate hardware failures for our controller tier and our hypervisor tier and it is assumed there will be network availability for this project that is outside the scope of this project. The customer may request support by opening a ticket via Metacloud's support website, email, or by calling Metapod support.
WebEx	WebEx Maintenance Window is 7 p.m. - Midnight Pacific Time nightly. Services will be available on alternate meeting site while primary site is updated.
Spark	We notify all customers of any downtime that affects them and schedule downtime according to their schedules.
Cloud Email Security	From time to time, Cisco performs scheduled maintenance to update the servers (Cisco and third-party servers at the data center[s]) and software that are part of the Cloud Email Security service. Cisco will make all reasonable attempts to notify Customer at least 5 business days in advance of any planned downtime or scheduled maintenance. Notwithstanding the foregoing, Customer acknowledges that Cisco may, in certain situations, need to perform emergency maintenance on less than 48 hours advance notice.
Cloud Web Security	From time to time, Cisco performs scheduled maintenance to update the servers (Cisco and third-party servers at the data center[s]) and software that are part of the Cloud Email Security

Cisco Cloud Offering	Response
	service. Cisco will make all reasonable attempts to notify Customer at least 5 business days in advance of any planned downtime or scheduled maintenance. Notwithstanding the foregoing, Customer acknowledges that Cisco may, in certain situations, need to perform emergency maintenance on less than 48 hours advance notice.
Meraki	The Cisco Meraki cloud runs on a redundant data center design and therefore does not require scheduled downtime. However, if scheduled downtime is ever required, customers will be notified via email and via a banner in the Meraki dashboard.
Tropo	We notify all customers of any downtime that affects them and schedule downtime according to their schedules.
Cisco Energy Management	We notify all customers of any downtime that affects them and schedule downtime according to their schedules.
Cloud Consumption as a Service	Not applicable

8.12.7 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Cisco Response:

SLA remedies and consequences vary by cloud service offering. This requirement is more pertinent to an IaaS solution and as such our Metapod IaaS Private cloud model does offer such remedies as described below. For other cloud offerings, this requirement does not apply since the disaster recovery metric is embedded within the overall Availability metric. Please see Attachment 3 Service Descriptions and SLAs for further details on specific cloud offerings and the applicable SLA remedies.

Our Metapod cloud offering remedies are as follows:

- Service Credits are calculated as the number of days that Cisco may add to the end of the Term at no charge to End User for either a Control Plane or Data Plane outage (whichever was Unavailable) in the Availability Zone affected for the calendar month in the Unavailability occurred in accordance to the schedule below. If both the Control Plane and Data Plane were Unavailable, the lower of the Monthly Uptime Percentage will determine the Service Credit applied. End User must notify Cisco of any Unavailability for which End User is claiming Service Credits, including the following:
    - ❑ Services impacted and claimed Service Level failure
    - ❑ Any activities performed prior to the claimed Service Level failure
    - ❑ Business impact of service outage/disruption
    - ❑ Any other reasonably requested information pertaining to the claimed Service Level failure (i.e., support ticket #).
- Monthly Uptime Percentage — Service Credit

- Less than 99.99 percent but equal to or greater than 99.9 percent – 3 days
- Less than 99.9 percent but equal to or greater than 99.0 percent – 7 days
- Less than 99.0 percent – 15 days.

Cisco will begin measuring the Monthly Uptime Percentage 1 calendar month after the Availability Zone has been setup and End User has access to the environment. This period of time allows End User and Cisco to evaluate the Services are being performed as specified and the platform is operating according to the Documentation.

8.12.8 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.

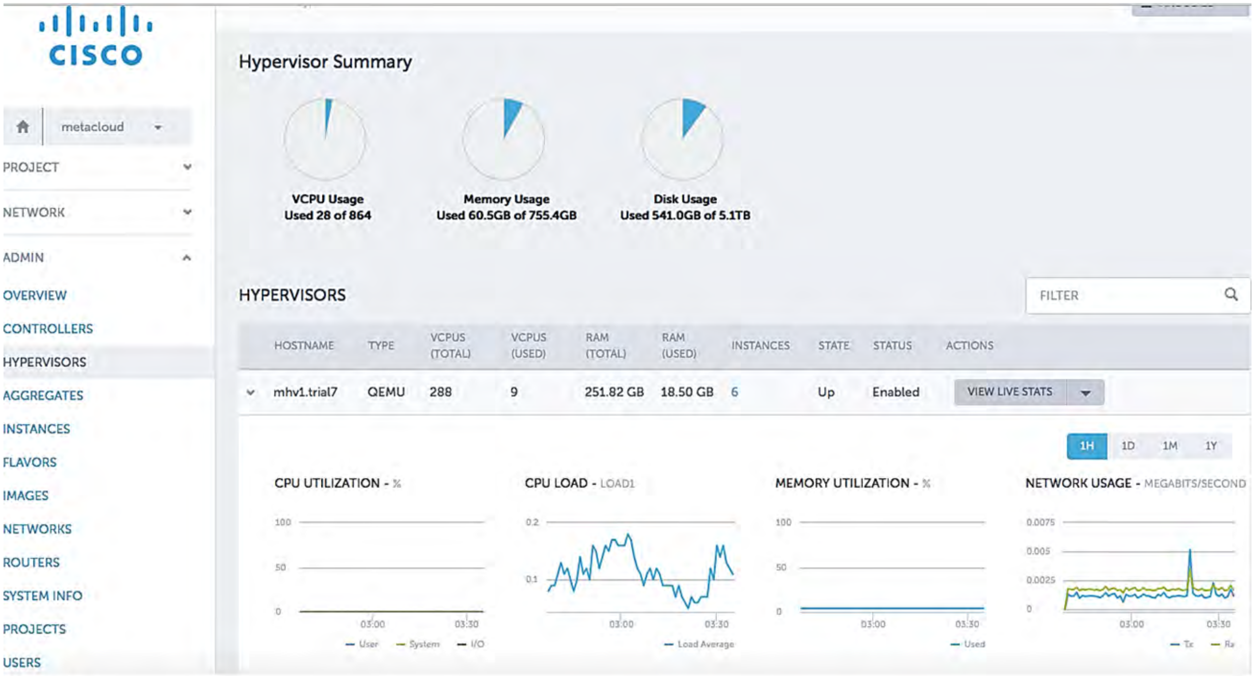
Cisco Response:

Table 29. Sample Performance Reports

Cisco Cloud Offering	Response
Metapod	Cisco provides trending reporting (performance included) through our metrics system. You can look at trending by the hour, day, month, or year on the key resources, including CPU, memory, network, and disk as well as other aspects of the system. The Cisco Metapod dashboard provides both live and historical statistics (Figure above and beyond the standard OpenStack Horizon dashboard features. These enhanced statistics are available for controllers and hypervisors for aggregate use and capacity, including CPU, memory, network, and allocated resources. The reports our dashboard provides include: ■ Performance (Availability KPI) ❑ Each AZ has been built with an HA framework around the orchestration which is designed for greater than 99.99 percent availability of OpenStack services. Based on our current customers, we are exceeding this expectation. ■ Capacity Management Evolution and Trend ❑ We provide weekly capacity and trend reports. The admin dashboard also provides reporting as well as live statistics. ■ Incident/Change ❑ We track all of our incidents and changes through our support portal (https://support.metacloud.com). ■ Asset Management (Physical/Virtual) ❑ We track the physical assets within the cloud and manage their uptime. Our platform provides tools for the client to track the virtual instances in the cloud either from the user or administrator point of view.

Cisco Cloud Offering	Response
	■ Component/Service Availability/Status ❑ As part of our monitoring, as well as our software platform architecture, we focus on service availability for all the OpenStack components that we run. We build an HA cluster for our controller tier and run all services within an HA framework. We have never had a complete outage based on our architecture. ■ Security Assessment (Compliance/Vulnerability) ❑ Security, process, and procedure controls are important components in the Cisco Managed Service offering. Cisco's development processes and system security are based upon industry best practices. Our clients are regularly conducting audits or systems security scans on our platform and we work with them to do so. ❑ Cisco provides weekly capacity reports that are based on overall usage as well as on-demand user and admin-generated reports. Cisco Metapod capacity reports are sent weekly and generated by the operations team. The administrator generates the trending metrics. Cisco Metapod capacity reports are in email format. The trending reports are graphics screens that are within the administrator's dashboard. Since each cloud platform is private to each client, the reporting is only available for the cloud it is running in and only accessible by the customer that owns that cloud. All access and user accounts are controlled by the customer, so reporting is inherently confidential.
WebEx	Activity and usage WebEx reports are available over the web as batch statistics.
Spark	New product offering. Not available at this time.
Cloud Email Security	CES performance reports are available from the administrative GUI available over the web. Near real time statistics are presented.
Cloud Web Security	CWS performance reports are available from the administrative GUI available over the web. Near real time statistics are presented.
Meraki	Performance reports are available in the Meraki dashboard.
Tropo	New product offering. Not available at this time.
Cisco Energy Management	CEM provides a web-based portal to view dashboards, obtain Device information, generate reports, and manage Policies.

Cisco Cloud Offering	Response
Cloud Consumption as a Service	Not applicable



Hypervisor Summary

VCPU Usage
Used 28 of 864

Memory Usage
Used 60.5GB of 755.4GB

Disk Usage
Used 541.0GB of 5.1TB

HYPERVISORS

HOSTNAME	TYPE	VCPUS (TOTAL)	VCPUS (USED)	RAM (TOTAL)	RAM (USED)	INSTANCES	STATE	STATUS	ACTIONS
mhv1.trial7	QEMU	288	9	251.82 GB	18.50 GB	6	Up	Enabled	VIEW LIVE STATS

CPU UTILIZATION - %

CPU LOAD - LOAD1

MEMORY UTILIZATION - %

NETWORK USAGE - MEGABITS/SECOND

3356p003/a

Figure 2. Metapod Historical Reporting Screenshot

8.12.9 Ability to print historical, statistical, and usage reports locally.

Cisco Response:

Table 30. Report Printing

Cisco Cloud Offering	Response
Metapod	All the reports described above (availability, statistical, usage, and others) can be printed locally.
WebEx	Yes
Spark	Using the detailed CDR you will be able to see and print all usage historically and statistically.
Cloud Email Security	Customers also can access a comprehensive support portal with an extensive knowledge base of subject matter expertise to assist with their needs. Using this support portal, customers can view all current and historical events/tickets, reports as well as the status of their cloud service infrastructure.

Cisco Cloud Offering	Response
Cloud Web Security	Yes reports can be printed.
Meraki	Usage reports are available in the Meraki dashboard.
Tropo	Using the detailed CDR you will be able to see and print all usage historically and statistically.
Cisco Energy Management	CEM provides a web-based portal to view dashboards, obtain Device information, and generate reports that can be printed.
Cloud Consumption as a Service	Not applicable

8.12.10 Offeror must describe whether or not its on-demand deployment is supported 24x365.

Cisco Response:

Yes, Cisco's offerings are supported 24x7x365.

8.12.11 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Cisco Response:

Table 31. Scale-up and Scale-down

Cisco Cloud Offering	Response
Metapod	Yes, the scaling up and down of the IaaS is available 24/365. Cisco Metapod is an elastic IaaS platform designed with the capabilities to scale up and scale down resources (Compute, RAM, Storage, VM) depending on the application architecture, hardware resources, and PaaS layer. Elasticity in the context above, typically resides on the cloud administration or user side of the demarcation point of the system. If, on the other hand, we need to scale up the physical hardware hypervisor pool, we make it very simple for our customers to add capacity. They merely submit a support ticket asking for additional hardware to be added, and our operations team will bring that new hardware into the existing cloud. Cisco has enhanced the user interface of the Horizon dashboard and provides the cloud administrator much greater control to manage a large number of hypervisor systems and multiple availability zones. Our system provides reports to both the users and admins on use of key resources such as CPU, memory, and disk. Users get a view of their project and usage against quota; administrators get a view of the overall utilization on a per-tenant basis. Custom reports can be run for specific time periods. We also offer cloud metrics, which give you a graphical view over time of key resources. The Cisco solution provides a zero-touch self-service environment for your users. VM operations such as creation, networking, storage, and load-balancer configurations are

Cisco Cloud Offering	***Response***
	decentralized and configurable via the tenant users themselves. Networking has been simplified and optimized for the users, such that no complicated virtual topologies need to be designed by them; they merely launch VMs. VMs will be attached to a Layer 2 VLAN, assigned a private IP address from the CIDR block associated to that VLAN, be associated with a DHCP server and Gateway, all automatically. Storage is consumed in much the same way in that the tenants merely select the available storage originally made available to them by system administrators, and they can then associate it with their VMs. Users can launch, configure, and control their own load balancers, CPU, memory, and storage, which are enabled by default in Cisco Metapod.
WebEx	Scale up and scale down are built in to the application environment and are available in accordance with the SLA.
Spark	Scale up and scale down are built in to the application environment and are available in accordance with the SLA.
Cloud Email Security	Scale up and scale down are built in to the customer application environment and are available in accordance with the SLA.
Cloud Web Security	Scale up and scale down are built in to the CWS environment and available 24x365.
Meraki	The Meraki cloud can be scaled up or down 24x7x365.
Tropo	Scale up and scale down are built in to the application environment and are available in accordance with the SLA.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.13 (E) CLOUD SECURITY ALLIANCE QUESTIONNAIRES

Describe your level disclosure of compliance with CSA Star Registry for each Cloud solutions offered.

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5
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.

Cisco Response:

Cisco has completed the Self-Assessment as described in Section 5.5.5 and is attached accordingly as part of the completed Attachment 9 Cisco Exhibit_1_to_Attachment_B_-_CAIQ.

8.14 (E) SERVICE PROVISIONING

8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Cisco Response:

Cisco will accommodate rush orders on a best effort basis. Some Cisco products/services can be delivered next day from our distribution center within the United States.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Cisco Response:

Typically, once the customer signs the purchasing agreement and the infrastructure is in place Cisco will deploy the cloud in less than 30 days. We typically achieve two weeks for deployment but it really depends on the level of integration with customer environment. Cisco will accommodate rush orders on a best effort basis.

8.15 (E) BACK UP AND DISASTER PLAN

8.15.2 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

8.15.3 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

8.15.4 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.

Cisco Response:

Table 32. Backup and Disaster Plan

Cisco Cloud Offering	*Response*
Metapod	Disaster recovery for on premise clouds are typically performed by our clients; they own the VM instances as well as the application data and have the most knowledge of the needs. Swiftstack Object storage is used as a solution for OpenStack backups for virtual machines and their data. Most of our customers use a higher level orchestration system either built in house or using standard tool sets (e.g., Chef, Puppet, Ansible, Cloud Foundry, RightScale, Cliqr) to build or redeploy a DR landing zone should a disaster occur. This is generally tied into the application as well, where it can perform auto healing based on the types of behavior it sees in the infrastructure. If, however, a further disaster recovery is necessary, the broader Cisco organization can absolutely help the customer develop a five nines DR apparatus using hardware based load balancers, balancing across physically disparate availability zones to software based load balancers controlling the web, app, and DB tiers. This would be based on the customer architecture requirements and can be handled as part of the broader cloud solution. In order to make images available across multiple availability zones, the OpenStack glance image service can be backed by the swift object storage and implemented on a swiftstack object

Cisco Cloud Offering	Response
	storage cluster. The backup storage resides on swiftstack object storage clusters installed on dedicated UCS compute platforms in a location indicated by the customer. Backup can also be performed on public cloud services (i.e., Iron Mountain or Amazon S3). The Metapod OpenStack solution is installed on the customer premise or in any colocation facility preferred by the customer. Service Credits are calculated as the number of days that Cisco may add to the end of the Term at no charge to End User for either a Control Plane or Data Plane outage (whichever was Unavailable) in the Availability Zone affected for the calendar month in the Unavailability occurred in accordance to the schedule below. If both the Control Plane and Data Plane were Unavailable, the lower of the Monthly Uptime Percentage will determine the Service Credit applied. End User must notify Cisco of any Unavailability for which End User is claiming Service Credits, including the following: ■ Services impacted and claimed Service Level failure ■ Any activities performed prior to the claimed Service Level failure ■ Business impact of service outage/disruption. Any other reasonably requested information pertaining to the claimed Service Level failure (i.e., support ticket #). Monthly Uptime Percentage — Service Credit. Less than 99.99 percent but equal to or greater than 99.9 percent — 3 days. Less than 99.9 percent but equal to or greater than 99.0 percent — 7 days. Less than 99.0 percent —15 days. Cisco will begin measuring the Monthly Uptime Percentage 1 calendar month after the Availability Zone has been setup and End User has access to the environment. This period of time allows End User and Cisco to evaluate the Services are being performed as specified and the platform is operating according to the Documentation. Cisco Metapod is deployed at customer premises. DR risks and mitigation strategies can be discussed with the purchasing entity once location and site is known. Cisco Metapod is deployed at customer premises, typically over several availability zones (Metapod deployments) located in different premises.
WebEx	WebEx's Global Site Backup (GSB) system ensures that you experience business continuation even in a disaster situation. Additional benefits include full redundancy for maintenance

Cisco Cloud Offering	Response
	windows or other system outages. GSB provides each customer with a backup WebEx site. The GSB system provides real-time, two-way database data synchronization between the primary site and the backup site. All customers are supported with GSB. Cisco WebEx can provide APIs to the Purchasing entity to manage provisioning of personnel or recording retention management. Internet must be available.
Spark	Backup and disaster recovery are built in to the application environment and are available in accordance with the SLA. This is a new offering and therefore the requested information is proprietary at this time. Cisco will be willing to share this information upon request following award.
Cloud Email Security	CES is operated in redundant data centers in the east and west of the United States. Each of our data centers has multiple levels of redundancy built into its infrastructure. The first is the network infrastructure, which has multiple carrier-grade access routers, distribution switches, and Point-of-Delivery (PoD) switches, so there is no single point of failure. Behind this highly redundant networking infrastructure, multiple dedicated Cisco hardware units are used for email processing, reporting, tracking, and more. To prevent failure and to maintain connectivity in the event of an unexpected incident, the data centers use two physically separated fiber inputs. Additionally, these data centers have the bandwidth capacity to process up to 20 Gbps of network traffic. Most data centers today must cope with severe issues resulting from the improper management and control of equipment-generated heat. Cisco data centers are constructed following the most advanced designs for space and power in the industry. They have 100 percent power availability, delivered through a sophisticated grid architecture that includes primary circuits and failover connections, both of which come from two completely separate N+2 power systems. Each of these systems has separate Uninterruptible Power Supply (UPS) batteries, generators, Power Distribution Units (PDUs), and Remote Power Panels (RPPs), and are delivered to each rack through color-coded receptacles. This arrangement maintains consistent uptime for the email security infrastructure. As server densities increase, the demand on cooling systems grows significantly. Each Cisco data center facility has enough primary and backup cooling to dissipate the heat generated by the email security infrastructure and to provide ample cooling in case of a failure with one of the cooling systems. The cooling infrastructure is delivered through Freon, swamp, chilled-water,

Cisco Cloud Offering	Response
	and outside-air mechanisms.
Cloud Web Security	Retention periods for CWS traffic are 45 days for completed HTTP/S requests and 1 year for blocked transactions. Additional retention periods can be negotiated. CWS Data Centers are located in the following U.S. geographic areas: ■ Chicago ■ Dallas ■ Miami ■ San Jose ■ Secaucus ■ Washington, DC. CWS application and architectural elements are engineered to high degrees of fault tolerance and redundancy. Customers' accounts are implemented and managed to survive a complete data center failure with traffic failover to an alternative data center. **Minimum Data Center Facility Standards** For a data center facility to be considered as a location to host Cisco CWS equipment, the following is required: ■ Locked cages or cabinets ■ Onsite physical security provided by one or more of the following: ❑ Onsite security guard patrols ❑ Strategically positioned cameras ❑ Biometric/RFID access controls to critical areas ❑ Alarms to alert against unauthorized intrusions ■ Uninterrupted power source through one or more of the following: ❑ Physically diverse power feeds ❑ Diverse power utility companies ❑ Battery-powered uninterruptible power ❑ Onsite generator with re-fueling agreement supplies to maintain power until resumption of normal utility service ❑ Testing of backup power sources on full-load at least once a year ■ Sufficient HVAC capabilities with monitored temperature and humidity controls ■ The presence of fire and smoke suppression systems that are regularly maintained ■ 24x7x365 audited physical access to the facility for authorized Cisco CWS staff only

Cisco Cloud Offering	Response
	■ 24x7x365 remote hands and eyes by experienced engineers responding to requests from authorized Cisco CWS staff only.
Meraki	Cisco Meraki runs in geographically distributed, redundant data centers. A failure at any data center will not bring down the Meraki service. Customers are assigned an active data center where their dashboard is hosted with a hot standby hosted in a redundant data center. In the event of a failure at both data centers, customer's data is backed up to a third data center.
Tropo	Backup and disaster recovery are built in to the application environment and are available in accordance with the SLA. This is a new offering and therefore the requested information is proprietary at this time. Cisco will be willing to share this information upon request following award.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.16 (E) SOLUTION ADMINISTRATION

8.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts.

Cisco Response:

Table 33. User Account Management

Cisco Cloud Offering	Response
Metapod	The Purchasing Entity is in charge of managing the user accounts and their identity. While Metapod provides a robust user identity component, we also support integration with the internal AD solution to manage user access permissions, identity management, etc. Access and reporting based on AD groups and specific AD and local users.
WebEx	Purchasing Entity can provision accounts through an Identity provider using Single Sign On federation services (SAML 2.0)
Spark	IT teams can add features that use existing security policies, like Single Sign-On (SSO) and synchronizing to your corporate employee directory so that terminations get processed without further IT administration. SSO - Is setup to require company-approved passwords and authentication that adhere to your corporate security standards. Uses identity providers using the Security Assertion Markup Language (SAML) 2.0 and Open Authorization (OAuth) 2.0 protocol.

Cisco Cloud Offering	***Response***
Cloud Email Security	The Customer will be provided access by Cisco to a web-based interface to administer and report on the Services. Access to the interface is via a secure (HTTPS) website and is password-protected. The Customer may have multiple administrators for a single account. The Customer can request a unique login for each administrator and provide full access or read only privileges specific to each user. The interface enables the customer administrator to: ■ Review statistics of all malware stopped and other email content blocked ■ Create access restrictions and apply these to specific users or groups ■ Configure and schedule automated system reporting; and track email messages. Customers also can access a comprehensive support portal with an extensive knowledge base of subject matter expertise to assist with their needs. Using this support portal, customers can view all current and historical events/tickets, reports, as well as the status of their cloud service infrastructure.
Cloud Web Security	Complete details of CWS management and configuration are available in the configuration guides found at: http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html The Customer will be provided access by Cisco to a web-based interface to administer and report on the Services. Access to the interface is via a secure (HTTPS) website and is password-protected. The Customer may have multiple administrators for a single account. The Customer can request a unique login for each administrator and provide full access or read only privileges specific to each user. Customers also can access a comprehensive support portal with an extensive knowledge base of subject matter expertise to assist with their needs.
Meraki	Meraki customers are allowed to manage their own administrator accounts.
Tropo	IT teams can add features that use existing security policies, like Single Sign-On (SSO) and synchronizing to your corporate employee directory so that terminations get processed without further IT administration. SSO - Is setup to require company-approved passwords and authentication that adhere to your corporate security standards. Uses identity providers using the Security Assertion Markup

Cisco Cloud Offering	Response
	Language (SAML) 2.0 and Open Authorization (OAuth) 2.0 protocol.
Cisco Energy Management	CEM uses role-based administration based on Customer provided data and map(s).
Cloud Consumption as a Service	Not applicable

8.16.2 Ability to provide anti-virus protection, for data stores.

Cisco Response:

Table 34. Anti-Virus Protection

Cisco Cloud Offering	Response
Metapod	Cisco Metapod does not include an anti-virus component for the data stored. This typically falls under the responsibility of the customer.
WebEx	Cisco WebEx manages anti-virus protection.
Spark	All Cisco data centers use AV protection for its offerings.
Cloud Email Security	AV protection on transient email (traffic) is a feature of the CES solution.
Cloud Web Security	AV protection on transient Web (traffic) is a feature of the CWS solution.
Meraki	All Meraki data centers use anti-virus protection.
Tropo	All Cisco data centers use AV protection for its offerings.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

Cisco Response:

Table 35. Data Migration

Cisco Cloud Offering	Response
Metapod	Cisco Advanced Services will create an offer based on specific migration requirements. This is not part of the Cisco Metapod offer but is a separate offer that our professional services team will make after defining the statement of work for the migration.
WebEx	Recordings can be migrated via .WRF files; contact lists
Spark	Data can be securely exported. If the Subscriber terminates the

Cisco Cloud Offering	Response
	Service for convenience (as allowed under the Spark Terms of Service, and effective upon expiration or termination of all outstanding Orders), the organization's Business Messaging account will be converted to the entry level, no-cost Business Messaging offer ("Free Spark"). The Storage included with Free Spark will be 5GB per User, but may not be pooled amongst Users. Additional terms applicable to Free Spark are set forth in the Spark Terms of Service.
Cloud Email Security	Migration services from CES will be limited to configuration settings of the customer environment in XML format.
Cloud Web Security	CWS migration services from CWS will not be available. Cisco will delete the account of each customer that migrates from the service.
Meraki	Network management data can be exported from Meraki devices and the Meraki cloud.
Tropo	Not applicable
Cisco Energy Management	Data can be securely exported. Customer understands and acknowledges that it is solely and fully responsible for backing-up and/or otherwise protecting its own data against loss, damage, or destruction.
Cloud Consumption as a Service	Not applicable

8.16.4 Ability to administer the solution in a distributed manner to different participating entities.

Cisco Response:

Table 36. Distributed Administration

Cisco Cloud Offering	Response
Metapod	Cisco Metapod is a multitenant and offer the customer the possibility of creating and managing different tenants. It provides the needed isolation from a network perspective. It also uses role-based access to provide access to the different tenants within the system. Administrators (from the Purchasing Entity) are responsible for creating policies, create VM "flavors", define quotas and policies, etc.
WebEx	Different participating entities would need to be defined as separate org groups. They can not be considered as separate sub groups in an organization when there are differing configuration/rules requirements.
Spark	Cisco Spark is a multitenant and offer the customer the

Cisco Cloud Offering	Response
	possibility of creating and managing different tenants.
Cloud Email Security	Each customer will have the ability to manage delivery to sub-domains or designated SMTP destinations per applied policy.
Cloud Web Security	Each customer will have the ability to manage delivery to sub-domains or designated sub-destinations per applied policy.
Meraki	Meraki customers are allowed to manage their own administrator accounts including adding third parties as administrators.
Tropo	Cisco Tropo is a multitenant and offer the customer the possibility of creating and managing different tenants.
Cisco Energy Management	CEM customers are allowed to manage their own administrator accounts including adding third parties as administrators.
Cloud Consumption as a Service	Not applicable

8.16.5 Ability to apply a participating entity's defined administration polices in managing a solution.

Cisco Response:

Table 37. Participating Entities Admin Policies

Cisco Cloud Offering	Response
Metapod	Cisco Metapod environment will take and apply policies defined by the participating entity.
WebEx	Only works if separate WebEx site is created.
Spark	IT teams can add features that use existing security policies, like Single Sign-On (SSO) and synchronizing to your corporate employee directory so that terminations get processed without further IT administration. SSO - Is setup to require company-approved passwords and authentication that adhere to your corporate security standards. Uses identity providers using the Security Assertion Markup Language (SAML) 2.0 and Open Authorization (OAuth) 2.0 protocols. Directory synchronization - Real-time management of employee lifecycle changes with Microsoft Active Directory helps to ensure that former employees can't access your company data using the Cisco Spark app.
Cloud Email Security	Policy configuration will be managed during the initial implementation of the service.
Cloud Web Security	Policy configuration will be managed during the initial implementation of the service.
Meraki	Customers are allowed to create their own policies around

Cisco Cloud Offering	Response
	administrative accounts.
Tropo	IT teams can add features that use existing security policies, like Single Sign-On (SSO) and synchronizing to your corporate employee directory so that terminations get processed without further IT administration. SSO - Is setup to require company-approved passwords and authentication that adhere to your corporate security standards. Uses identity providers using the Security Assertion Markup Language (SAML) 2.0 and Open Authorization (OAuth) 2.0 protocols. Directory synchronization - Real-time management of employee lifecycle changes with Microsoft Active Directory helps to ensure that former employees can't access your company data using the Cisco Tropo app.
Cisco Energy Management	EMaaS controls energy management of Devices through Policies. Policies are used to automate power management of Devices, according to the parameters set by the Customer. Each Policy must have at least one condition and one action in order to be triggered and executed. These Policies can be time, event, or location based.
Cloud Consumption as a Service	Not applicable

8.17 (E) HOSTING AND PROVISIONING

8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Cisco Response:

Table 38. Cloud Hosting Provisioning Processes

Cisco Cloud Offering	Response
Metapod	Cisco Metapod provides a complete logging of the provisioning of resources and this can be used for documentation of provisioning processes.
WebEx	Not applicable to SaaS offering
Spark	There are two ways to add users to your organization: ■ Manually entering the users' email addresses as a comma separated list. ■ Synchronizing to your Active Directory. To quickly get started, you can add key people in your organization, like support personnel, by manually using their email addresses. Then, expand the number of people that you add later using directory synchronization.

	Setting up Active Directory synchronization with Cisco Directory Connector is an option to consider if your organization has more than 50 users. Directory Connector queries your Active Directory to retrieve users and groups and to sync to the Connector service. ■ When you add a user entering their email address, their email address in Cisco Cloud Collaboration Management and Active Directory must exactly match for the accounts to be linked. ■ Any time you add or delete users from your Active Directory, they are automatically added and deleted from your organization in Cisco Cloud Collaboration Management. This saves you time and helps you comply with security requirements. Note that Active Directory synchronization does not support group management. ■ After you add users using Active Directory synchronization, you'll need to edit their services to enable licensed features.
Cloud Email Security	Not applicable to SaaS offering
Cloud Web Security	Not applicable to SaaS offering
Meraki	Cisco Meraki is a cloud based network management solution.
Tropo	Not applicable
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

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.)

2. Creating and storing server images for future multiple deployments

3. Securing additional storage space

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).

Cisco Response:

Table 39. Tools

Cisco Cloud Offering	Response
Metapod	Cisco will perform the process of provisioning of a new server (at customer request) in Metapod’s OpenStack. This comes at no additional cost. Customer (or a third party) is responsible to physically rack the server, wire it, and communicate in advance

Cisco Cloud Offering	Response
	the scheduled maintenance window. Cisco Metapod team is responsible for creating and storing server (hypervisor) images for multiple future deployments. Customer is responsible for the creation and storage of guest operating system images for future multiple deployments. Cisco Metapod is an on-premises Private Cloud deployed on customer hardware. Cisco will proactively signal the customer when capacity thresholds in storage space are reached and help the customer to plan for addition of new storage capacity. The customer will perform the physical addition of the capacity (disks) and Cisco will perform the software (orchestration) provisioning of it. Monitoring tools are part of the Metapod cloud software. We have more than 100 monitoring probes in the Metapod software. Customer can interact with the tools and create reports of real time, historical, and statistical data in the Private Cloud.
WebEx	Not applicable to SaaS offering
Spark	Chef is utilized for configuration management.
Cloud Email Security	Not applicable to SaaS offering
Cloud Web Security	Not applicable to SaaS offering
Meraki	Provisioning and managing additional devices is done by claiming Meraki order numbers.
Tropo	Chef is utilized for configuration management.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	Not applicable

8.17.3 Ability to provide IaaS, PaaS, and SaaS solutions as defined service offerings with established rate structures

Cisco Response:

Cisco has been and will continue to provide industry leading cloud solutions as defined IaaS, SaaS, and PaaS per NIST with an established rate structure per the Cisco U.S. Global Price List.

8.18 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)

Describe your testing and training periods that your offer for your service offerings.

Cisco Response:

Table 40. Trial And Testing Periods

Cisco Cloud Offering	Response
Metapod	Cisco Metapod offers a trial environment hosted by Cisco as well as the possibility to run a more customer-specific trial on premises. The Cisco hosted trial pod provides full access to creating VMs and API access in order to test DevOps tools or applications accessing the APIs. In the trial environment, the Solution Architect has admin access to train or do anything admin related on behalf of the customer. Typically, we can provide a limited number (~10) of floating (public IPs) and as many private IP addresses as needed. Normally, we provide these trials for 2 weeks, but we can extend upon request. Customer Admin has the right to define projects (tenants).
WebEx	Cisco provides a 14 day free trial.
Spark	Cisco provides a free Cisco Spark account. This is how you get access to 24x7 support in the #SparkDen. We're around to assist via email or in a Spark room full of helpful resources. Use the same account you have for your Cisco Spark app.
Cloud Email Security	Testing is available for each customer, up to 90 days.
Cloud Web Security	CWS trial accounts can be configured and created for customers upon request, typically these trials last 30 to 60 days.
Meraki	Cisco Meraki provides free trials to any customer interested in the solution. Trials are limited to 60 days, but can be extended if requested by a customer.
Tropo	Development is always free on Tropo.com. Signup for an account and start developing your application.
Cisco Energy Management	Measure energy consumption for up to 1,000 network devices throughout your distributed office or data center. Set policies to start saving energy, costs, and carbon. Try Cisco Energy Management software or Cisco Energy Management Cloud free for 21 days.
Cloud Consumption as a Service	Cloud Consumption as a Service provides 30 days of portal usage free-of-charge to: ■ Reduce cloud, privacy, and compliance risks, and protect the company's brand and intellectual property. ■ Deliver cloud services faster to meet lines-of-business' needs. ■ Simplify cloud management with the right people, process, and tools. ■ Reduce your cloud costs up to 15 percent by

Cisco Cloud Offering	Response
	consolidating cloud services. ■ Improve service performance by foreseeing infrastructure impact. Within the 30 day trial period, Cisco provides full support in using the CCaaS Portal and Features. A step-by-step guide for setting up the free trial account is provided for customers too.

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.

Cisco Response:

Table 41. Test and/or Proof of Concept

Cisco Cloud Offering	Response
Metapod	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
WebEx	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Spark	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Cloud Email Security	CES POC environment for evaluation is available per the process available from the Cisco Global Security Sales Organization or is available electronically from https://info.sourcefire.com/ContentSecurityOfferPage.html
Cloud Web Security	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Meraki	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Tropo	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Cisco Energy Management	Our trial program is used by the vast majority of our customers to run a test and/or proof of concept environment for evaluation.
Cloud Consumption as a Service	Cloud Consumption as a Service provides a 30-day free-of-charge trial period to access the Cloud Usage Portal. Customers can access it by using a Cisco Connection Online accounts. After the 30 day trial period, the customer can purchase licenses required to use the SaaS, or can decide to close their accounts. The use of 30-day free trial creates no obligations for the customer.

8.18.3 Offeror must describe what training and support it provides at no additional cost.

Cisco Response:

Table 42. Training

Cisco Cloud Offering	Response
Metapod	Metapod provides a remote half-day “Introduction to Metapod” training at no cost for each new Availability Zone to be deployed. Support services are included in the cost of the Metapod licenses.
WebEx	Support is available from Cisco TAC and is available as part of the licensed feature set at no additional cost. Training is available from Learning@Cisco or its partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee. Some offerings, such as Meraki, may provide free training on how to use and deploy their specific products, potentially including training videos, website content, and documentation.
Spark	Support is available from Cisco TAC and is available as part of the licensed feature set at no additional cost. Training is available from Learning@Cisco or it's partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee. Some offerings, such as Meraki, may provide free training on how to use and deploy their specific products, potentially including training videos, website content and documentations.
Cloud Email Security	Support is available from Cisco TAC and is available as part of the licensed feature set at no additional cost. Training is available from Learning@Cisco or it's partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee
Cloud Web Security	Support is available from Cisco TAC and is available as part of the licensed feature set at no additional cost. Training is available from Learning@Cisco or it's partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee
Meraki	Training can be provided to customers by request.
Tropo	Support is available from Cisco TAC and is available as part of the licensed feature set at no additional cost. Training is available from Learning@Cisco or it's partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee. Some offerings, such as Meraki, may provide free training on how to use and deploy their specific products, potentially including training videos, website content and documentations.
Cisco Energy	Support is available from Cisco TAC and is available as part of

Cisco Cloud Offering	Response
Management	the licensed feature set at no additional cost. Training is available from Learning@Cisco or it's partners for a fee. Administrative manuals and documentation are available at Cisco.com for no additional fee. Some offerings, such as Meraki, may provide free training on how to use and deploy their specific products, potentially including training videos, website content and documentations.
Cloud Consumption as a Service	The CCaaS is very simple and intuitive to use. However, basic support in using the Portal and Features will be provided at no additional cost for the 30 days trial period.

8.19 (E) 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.

Cisco Response:

Table 43. Integration

Cisco Cloud Offering	Response
Metapod	We offer a standard OpenStack API for higher level applications to integrate. **PaaS:** Cisco supports our customers in deploying and operating a wide range of application platforms inside their virtual machines. With regards to PaaS, there is well documented community and commercial support in OpenStack available for popular PaaS platforms such as CloudFoundry (http://docs.cloudfoundry.org/deploying/openstack/) and OpenShift (http://docwiki.cisco.com/wiki/OpenShift_Origin_Heat_Deployment_Guide). Cisco OpenStack uses the standard OpenStack APIs and exposes all deployed APIs to end users of the private cloud to ensure out-of-the-box integration with popular tools and platforms. In addition, Cisco regularly provides architecture and platform guidance to our customers to help them select and implement the right application platform for their needs. **Integration into log analysis tools** Cisco can configure things like Syslog and point them to specific [Customer] tools and, as an extension of the [Customer] IT team, will work to integrate into pertinent and appropriate tools to further smooth operations of the cloud. Consumption Reporting Cisco has referenceable customers that have used our Nova Usage API to create an easily integrated charge-back portal for the tenant community of the cloud. Thus, (Customer) can easily figure out the private cloud cost that they are operating and then, through cloud cruiser APIs, integrate that into whatever output is supported. Thus, integration is doable and something Cisco will work as an extension of the (Customer) IT team to bring to fruition. Cloud Cruiser leverages OpenStack; therefore, Cisco with the

Cisco Cloud Offering	Response
	standard APIs that are inherent with an OpenStack distribution is functional. http://www.cloudcruiser.com/partners/openstack/ **Service authorization** Our system supports an administration role that can control users, quotas, authentication, and overall see accounting on per-tenant basis. The accounting can be seen in the overview option of the project/tenant menu. In addition, we support project-based administration through our own Cisco self-service enhancement, which means a user can become the administrator of their own project and control access to those resources. When combined with Active Directory or LDAP integration, it can provide a zero-touch self-service environment for your users. **Hybrid Cloud tools** For customers that choose to have a mixed Public and Private environment, we integrate with popular OpenSTack compatible tools (CliQr, Scalr, etc.), as well as with Cisco Intercloud Fabric for business. These tools provide platform independence, application mobility on different platforms (Metapod, Amazon, Microsoft Azure, etc.). There are many other points of integration with Cisco Metapod and we are ready to discuss them case by case. Also, we provide a standard OpenStack API so all the tools compatible with that will be compatible with Cisco Metapod Private cloud.
WebEx	Yes, standard APIs are available for Single Sign on.
Spark	We offer a standards base REST api and scripting API that allows you rot add communications (voice and SMS) into any application.
Cloud Email Security	CES can be integrated to an existing customer infrastructure and workflow using directory integration over secure LDAP and SMTP interfaces to other email work flows.
Cloud Web Security	CWS can be integrated to an existing customer infrastructure and workflow using directory integration over secure LDAP and SMTP interfaces to other email work flows.
Meraki	Cisco Meraki supports many APIs including an external captive portal API, wifi location analytics API, provisioning API, SNMP, syslog, and RADIUS.
Tropo	We offer a standards base REST api and scripting API that allows you rot add communications (voice and SMS) into any application.
Cisco Energy Management	Not applicable
Cloud Consumption as a Service	The current version of the CCaaS application does not support standard based interface to support additional integration. However, this item is on the roadmap for implementation within the next 6 months.

8.19.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Cisco Response:

Table 44. Customization and Personalization of Solutions

Cisco Cloud Offering	*Response*
Metapod	Cisco Metapod team is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers.
WebEx	Cisco is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers. Webex has options to customize configuration flexibility of password rules, lockout and timeout confirmation settings, etc.
Spark	Cisco is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers.
Cloud Email Security	CES can be integrated to an existing customer infrastructure and workflow using directory integration over secure LDAP and SMTP interfaces to other email work flows.
Cloud Web Security	Cisco is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers.
Meraki	The configuration of Cisco Meraki devices is completely customizable to meet the needs of customers.
Tropo	Cisco is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers.
Cisco Energy Management	Cisco is open to discuss potential customization and personalization of our service. In fact we are doing this regularly for our customers.
Cloud Consumption as a Service	Not Applicable

8.20 (E) MARKETING PLAN

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Cisco Response:

The Cisco marketing plan includes three levels of marketing outreach:

1. **Cisco Sales Support**: Cisco has dedicated account teams assigned to all vertical segments across the State, Local and Education markets in U.S. Public Sector. These are highly experienced professionals in selling Cisco solutions to State agencies and political subdivisions, including cities, counties, municipalities, and public K-12 and higher education. They are also trained to market and promote the use and adoption of the

Cisco's direct contracts, particularly our NASPO ValuePoint contracts, which have been hugely successful for Cisco and convenient buying vehicles for our joint customers.

2. **Cisco Certified Reseller Communities**: In addition to the Cisco Sales teams, we intend to multiply customer adoption of the awarded contract through use of our extensive reseller community. As stated above, Cisco intends to vet, select and onboard for each executed Participating Addendum Authorized Resellers who are qualified and hold the required certifications and specializations to sell and support Cisco's cloud solution offerings. Cisco will work closely with the Authorized Resellers to provide marketing support as well as require them to execute demand generation activities to educate and promote the awarded contract.

3. **Cisco Marketing Support**: As a global technology solution provider, Cisco has numerous marketing programs and resources that support customer outreach and marketing, including channels promotions that provide incentives for the Authorized Resellers. Cisco also has a dedicated, highly seasoned U.S. Public Sector contracts marketing team that works closely with the Cisco contract managers to develop and execute a "Go-Live" contract marketing plan as well as ongoing marketing activities during the term of each contract, including but not limited to, email blasts and collateral marketing materials (i.e. flyers, postcards, etc.).

   In addition, Cisco will work with NASPO ValuePoint and the Authorized Resellers during the term of the contract to identify opportunities and new ways to promote the contract (i.e. conferences, meetings, tradeshows, etc.) for each calendar year. Subject to the approval of NASPO ValuePoint, the following are some examples of marketing and demand generation activities that Cisco, at its sole discretion, may execute for the new contract:

   - Media Outreach
     - Cisco has a PR team engaged to seek visibility with trade journals, and national and local press.
   - Coordinated Social Media Promotion
     - Cisco Blogs
     - Facebook
     - Twitter
     - LinkedIn.
   - Cisco Customer Newsletter with an article highlighting the contract (Quarterly).
   - Direct Email Outreach
     - Identify Targeted Audience (working in conjunction with industry publications, list purchases and/or utilizing our own customer base)
     - Email series.
   - Collateral
     - Brochures

- ❑ FAQ
    - ❑ Email template(s).
- ■ Tradeshow and local Conference Participation
    - ❑ Create flyers for distribution at Conferences, Tabletops, and other Events
    - ❑ URL Business Cards (create new cards to drive people to the site for more info)
    - ❑ Webinars.
- ■ Promotions
    - ❑ From time to time, Cisco may, at its sole discretion, have limited-time promotions for its resellers for certain technologies, which in turn, the resellers may, at their sole discretion, pass such savings to the eligible buyers. In addition, Cisco may, at its sole discretion, from time to time, offer for limited time only (with applicable restrictions) certain equipment (i.e., SKUs) at reduced prices. Under such promotions, eligible buyers would be able to purchase such equipment at reduced list prices and would still be entitled to the contract price discount percentage(s) of the list prices as set forth in the Master Agreement.

8.21 (E) 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.

Cisco Response:

Cisco Services for Cloud Strategy, Management, and Operations

Delivered by Cisco and our Cisco Certified Partners, service engagements result in measurable business gains for our customers, who have achieved benefits such as 30 percent lower infrastructure costs, 50 percent faster disaster recovery, and 90 percent reduction in deployment time.

As part of our comprehensive cloud portfolio, Cisco Services offer a wide range of customer options including cloud visibility and risk management (Cloud Consumption), to overall strategy (Cisco Domain Ten workshops). We also offer secure and managed implementation services (Cloud Security Services, Services for Building and Adopting Cloud; Cloud On-Boarding Acceleration) while maintaining consistency with open standards (Cisco Services for OpenStack) and freeing IT from vendor management for troubleshooting (Solution Support for Critical Infrastructure).

- ■ **Cisco Cloud Consumption Services** address the challenges of Shadow IT. The service is software-enabled and provides an analysis of a customer's cloud usage, risk profile, and identifies cloud spend. The service is a software-enabled professional service that harnesses network intelligence to help customers determine which Cloud Service Providers (CSPs) are being accessed by employees across their entire organization. It provides full visibility into authorized and unauthorized (Shadow IT) public cloud usage, enabling informed decisions to manage risks and manage costs, resulting in business agility. The services include cloud consumption discovery, cloud usage assessment report, and one of cloud management or cloud maturity workshops.

- **Cisco Cloud Enablement Services for Adopting Clouds** accelerate planning and adoption of a public cloud environment; enable enterprises, commercial, and public sector customers to optimize their existing infrastructure to realize the full benefits of a public cloud; and facilitates Service Providers (SPs) to resell their services to help customers adopt cloud services offered by SPs. These services ensure successful adoption of cloud services and applications that help increase business benefits and ensure a seamless experience for your stakeholders.
- **Cisco Cloud Enablement Services for Building Clouds** provide strategy, planning and design, implementation, and optimization to meet the customer's unique public, private, and hybrid cloud requirements. This comprehensive set of services covers the major aspects of designing, building, and operating a public, private, and hybrid cloud; accelerates the planning and deployment of clouds; and enables service providers to provide secure clouds to their enterprise and public sector customers.
- **Cisco Cloud Enablement Services for Disaster Recovery as a Service (DRaaS)** allow the customer to re-establish operation of business critical operations after a major event such as fire or flood. The services consist of a number of optional components that assist with recovery in the context of company's established Business Continuity Program (BCP).

  The service options include Plan services (such as Business Impact Analysis [BIA], BIA Assessment, BIA Application Mapping, Disaster Recovery [DR] Risk Assessment, DR Architecture Assessment, DR Reference Architecture, DR High Level Design, DR Low Level Design), as well as Manage Service (DR Optimization). Cloud Enablement Services for DRaaS allow the service provider to deploy replication agents to replicate data and shadow virtual machines to allow accelerated Recovery Point Objective (RPO) and Recovery Time Objectives (RTO). The services span the entire lifecycle (Plan-Build-Run), and include DRaaS services for workshop, Strategy, Assessment, Validation, Design and Implementation, Customizations, and Managed Operation.
- **Cisco Cloud Enablement Services for InterCloud** allow IT leaders to holistically assess, plan, and manage hybrid cloud infrastructure. Implementation of an automation and integration framework is essential for successful hybrid cloud management. This umbrella portfolio of services for full lifecycle management results in business benefits of increased operational efficiency via end-to-end governance and reduced duplication; risk mitigation via seamless workload movement in hybrid cloud; and enhanced business decision impact via optimal placement of applications in the cloud.
- **Cisco Cloud Security Services** span the entire lifecycle (Plan-Build-Manage) of enterprise cloud and include Secure Cloud Strategy Workshop, IT GRC Strategy Service, Secure Cloud Provider Assessment, Network Device Security Assessment,

Secure Cloud Architecture PDI, Secure Cloud Technology PDI, Security Posture Assessment, and Security Optimization Service.

- **Cisco Consulting Services for Cloud** help you articulate your strategy and develop the business case and an architectural-led master plan for hybrid cloud, leveraging the best aspects of private cloud and public cloud resources. We work with you to assess the specific opportunity and benefits from cloud within your environment and to identify and prioritize critical business-impacting scenarios into an overall master plan – using tools and frameworks that we have developed and tested internally and with others.
- **Cisco Data Center Design and Deployment Service for Cisco Intelligent Automation for Cloud** addresses the need to break down technology silos and manage virtualized resources for realization of full potential of the cloud. Cisco IAC is a unified cloud management solution that offers policy-based automation, orchestration, and visibility across network, storage, server, and application stacks. It allows IT organizations to control and manage cloud-based services easily and transparently. Although IAC is easy to deploy and many companies do so on their own, Cisco understands that treating the shift to the cloud on a “learn as you go” process may introduce unnecessary risk and complexity which may affect business outcomes. For companies who prefer not to prepare for IT transition on their own, Cisco offers a set of services to help speed the deployment and implementation of IAC. By leveraging Cisco Services, organizations can take advantage of our deep knowledge base and key learnings from our existing customers.
- **Cisco Data Center Solution Support Service for Critical Infrastructure (new)** is an enhanced product support offer that provides customers with a single point of contact to manage support issues regardless of vendor. To support newly deployed cloud solutions, customers can use the Solution Support Service to contact Cisco directly and receive overarching, coordinated multi-vendor data center expertise, supplementing product support offers from Cisco and our technology partners.
- **Cisco Services for Cloud On-Boarding Acceleration** enable customers to develop a cloud migration strategy that manages the business risk and cost while accelerating time to ROI. The services analyze application dependencies, prioritize/validate applications for migration, and present a migration roadmap that includes TCO analysis. The service provides end-to-end project management and includes a workshop where a Cisco Services consultant uses the proprietary Cisco cloud migration methodology and acceleration service approach to confirm your business and technical requirements for application migration. The business benefits include business continuity due to smooth application transition, as well as improved application performance and agility.
- **Cisco Services for OpenStack** help customers in their deployment of OpenStack clouds. The new services are offered in these areas: Strategy and Assessment; Validation; Design and Deployment — software and application platform integration; and Optimization.

- ❑ The Strategy and Assessment services use Cisco's world-class experience in building clouds — witness Cisco's #1 ranking in IDC's 2013 Cloud Professional Services survey — and address the needs and requirements of our customers on their cloud journey.
- ❑ The Validation service provides an OpenStack environment for our customers to run development and pre-production environments, as well as help customers address critical next steps in their cloud journey.
- ❑ The Design and Deployment service provides our customers with production-ready system and infrastructure integration and helps customers develop specific OpenStack integrations and selected extensions.
- ❑ The Optimization service is targeted towards growing, maintaining, and evolving their OpenStack environments, as well as additional cloud application development assistance and OpenStack API integration.

- **The Cisco Domain Ten Framework** facilitates customers to understand the current state of their IT environment, desired state, and gaps. Cisco Domain Ten is a technology and vendor-neutral framework designed to assist with the identification and planning of any IT transformation.

8.22 (E) SUPPORTING INFRASTRUCTURE

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

Cisco Response:

Table 45. Infrastructure Required

Cisco Cloud Offering	*Response*
Metapod	Cisco Metapod can run on customer infrastructure (we define further our minimum requirements). Optionally, we can bundle the Metapod service (remote operation of the private cloud) with the infrastructure components (like UCS servers for OpenStack controllers and for the VM nodes, Nexus switches, and ASR routers). For customers willing to leverage their existent infrastructure, we have a set of minimum requirements defined here: OpenStack is an Infrastructure as a Service (IaaS) that allows for on-demand provisioning and snapshotting of Virtual Machines (VMs) including CPU, RAM, and storage. Other resources such as Layer 2 and Layer 3 networks can also be provisioned to segregate different tenants, called projects, from one another. The segregation is a part of the multi-tenancy capabilities of OpenStack. Cisco Metapod is a complete OpenStack distribution and contains the core components Nova, Keystone, Neutron, Glance, Cinder, Horizon, Heat, and soon to be Ceilometer. The

Cisco Cloud Offering	Response
	distribution has been optimized and hardened for production workloads. **Controllers** The foundation for any production ready OpenStack is a solid and robust architecture and it all starts with the controller tier, because it’s the controller nodes that run critical orchestration functions of the environment. The Horizon dashboard and API endpoints are also hosted on the controllers. In the Cisco Metapod architecture, the controller nodes run the OpenStack database and message queue server, which are clustered to ensure high availability. For each Availability Zone (AZ), three physical servers are configured to serve the controller role, and the loss of any of the controllers doesn’t affect the availability of the system (the controller tier is actually in an n+2 resiliency configuration). Pacemaker is used to form a quorum between the three controllers and to ensure consistency in these highly complex systems. Other technologies and techniques such as Corosync, HA proxy, and keepalive are used in this time-tested design and are among the many benefits of using Cisco Metapod. Another unique benefit of this design is that the platform supports the ability for In-Service Software Upgrade (ISSU) capabilities. In-place upgrades are supported without ever needing to rebuild the environment. The recommended server hardware configurations for the controllers are those that can support high IOP’s loads. This typically means fast x86_64 processors, fast memory, SSDs, and 10GigE networking. The ability to support VLAN tagging on the network ports is generally an additional pre-requisite (VXLAN support may require additional hardware requirements), but the configuration is non-prescriptive, suggesting minimum recommended performance levels. Here is the minimum recommended hardware configuration for the controller servers: ■ New generation motherboard ■ Lights Out Management (LOM) port ■ 2 x New generation CPUs with hyper-threading ■ Multi-core (e.g., Intel Xeon E5-2680 or better) ■ 192GB ECC RAM ■ 2 port 10GE NIC ■ Four or more system SSD disks (400GB or larger; for OS, logs, and stats). **Hypervisors** The compute/hypervisor nodes are the workhorses of the platform and support the actual guest instances. Cisco Metapod supports the “Group A” hypervisor, Qemu/KVM. The

Cisco Cloud Offering	Response
	Qemu/KVM hypervisor gets the greatest amount of testing and supports the largest amount of features. Much like the controllers in our solution, the Cisco Metapod hypervisors have been optimized with added stability, scalability, and simplicity features. Users have full control over instance type definitions including extra specs exposed via the dashboard. Live migrations and advanced VM placement algorithms are also supported. VM memory de-duplication via KSM enabled on the hypervisor allows for full hardware RAM utilization. From a server hardware perspective, the hypervisor nodes should reflect the requirements of the workloads, and much like with the controllers, Metapod is non-prescriptive. Here is the minimum recommended hardware configuration for the hypervisor servers: ■ New generation motherboard ■ Lights Out Management (LOM) Port ■ 2 x new generation CPUs with Hyper-threading and Virtualization extensions ■ Multi-core (e.g., Intel Xeon E5-2680 or better) ■ 256GB or more of ECC RAM ■ 2 port Intel 10GE NIC ■ 2 system SAS disks (500GB or larger; for OS, logs, and ephemeral root disks) ■ LSI MegaRAID JBOD/RAID 0 controller(s) for data disks ■ (Optional 8:1 ratio of HDD disks to SSD for non-ephemeral root disks and volumes via Ceph). **Storage** The variability in the configuration of the hypervisors comes into play depending on the storage requirements of the use cases. On one hand, customers have the option and flexibility of associating a NFS-based or other shared storage platform to the AZ. On the other hand, Cisco Metapod also has an optional storage feature, an open source platform called Ceph. Customers can choose to create a converged compute/storage server hardware platform with this option and by using server chassis that support a high density of drive bays. All of the available disks (OSDs) in the environment are aggregated together to form the block storage fabric. Ceph can be used for non-ephemeral root disk storage and for instance volume storage. The Cisco Metapod team will install and manage Ceph across the entire AZ. The two storage methods mentioned above can even be combined to create a hierarchical storage layout. **Network**

Cisco Cloud Offering	Response
	The network stack in a Cisco Metapod is as robust and highly available as all of the other components in the system, and it contains options that provide proven alternatives to what is available in upstream OpenStack. It is also flexible enough to integrate into several different data center network architectures; it has to be because few networks are alike. Like the other aspects of the platform, customers have options. The network stack in OpenStack is called Neutron, and it is built around a plugin architecture and supports various third-party plugins. For the Layer 2 networking, VLAN type networking is generally used in Cisco Metapod and the requirements for the switching layer are straightforward; basically support for VLAN trunking is needed. The Nexus 9000 series of switches are a common platform for this role. For Layer 3 networking, the standard upstream OpenStack Neutron reference platform generally outlines a single network node, but the Cisco Metapod architecture achieves resiliency through the use of complementary Cisco routing hardware and technologies. It supports the Cisco Aggregation Services Router (ASR) 1000 Series Neutron plugin to achieve the scalability, performance, and availability required to support production workloads. The Cisco Metapod controller nodes support many of the network controller functions, but with the integration of the ASR 1000 Neutron plugin, a pair of ASR 1000 routers can be used to specifically support the neutron-l3-agent functions including routing, Network Address Translation, and Floating IP address mapping. This best practices approach overcomes the limitations in basic OpenStack networking, while providing an alternative approach to propose advanced networking approaches like Distributed Virtual Routing (DVR).
WebEx	Cisco WebEx manages the Cloud Collaboration infrastructure.
Spark	The free Cisco Spark team collaboration app will continue to be available. Additionally, for ease of use, the user experience has also been extended and will be the primary interface for the newly added call and meeting functionality of the Cisco Spark service. This cloud offering will support calling from within the Cisco Spark application as well as Cisco 7800 and 8800 series desk phones. These endpoints will all be equipped with the latest Spark Phone OS software to enable simple cloud registration of endpoints. Cisco video meeting rooms as a service currently work with Cisco TelePresence SX10. Additional endpoints will be equipped with Spark Phone and Room OS (Operating System) cloud registration functionality soon. Message & Meeting capabilities require existing Call Control from Cisco (e.g. Cisco Unified Communications Manager, Cisco Business Edition, or Cisco Powered HCS

Cisco Cloud Offering	Response
	service)
Cloud Email Security	CES requires modification of existing customer DNS records. Access to policy configuration, reporting and management interfaces are over HTTPS browser based interfaces.
Cloud Web Security	Customers will need to direct their HTTP/S requests from their networks to the CWS service using either Cisco Connector technology supported by Cisco ASA/ISRG2/ISR4K/WSA or a Proxy Auto-Connect (PAC) file hosted either on the customer premise or in the CWS service. Customers who wish to use authentication to identify users will need to forward authentication using one of the connector methods available.
Meraki	Customers must purchase Meraki hardware (access points, switches, or security appliances) and applicable licenses for a functional solution.
Tropo	No new infrastructure is required. Customer are responsible for the proper functioning of their own web servers, software, applications, or services located outside of TROPO Data Center facilities.
Cisco Energy Management	A customer installed CEM Controller(s) on its network. Each Site deployment requires a minimum of one CEM Controller in the Customer's network. If .NET 3.5 is not present, it will automatically be downloaded as part of installation. Cisco also requires the following access to provide EMaaS: ■ IP routing and network access ■ Hostnames or IP addresses ■ SNMP RW access ■ SSH access ■ Enabled privilege ■ SNMP RO access.
Cloud Consumption as a Service	The Cloud Consumption as a Services consists of three components: 1. The Cloud Consumption as a Service SaaS Application 2. The Cloud Consumption Software Collector (optional) 3. Cloud Consumption professional Services (optional). Depending of the customer environment specifics (using a firewall or Web security gateway for URL Filtering (or not)), the customer may have a need to install the software collector. The collector software is a key component of Cisco's Cloud Consumption Service. It is designed to collect, process, and upload customer Internet traffic data to Cisco's Cloud Consumption Portal, where it can be viewed and analyzed. The Collector can process traffic data generated by supported Secure Web Gateways (SWG), Security Information and Event

Cisco Cloud Offering	Response
	Management products (SIEMs), Cisco Cloud Web Security (formerly ScanSafe), or NetFlow (v5 and v9). The Collector, which can be run from the command line or via a cronjob, takes network traffic data as an input, anonymizes the data, and masks all Source IPs and User Names in the data. This is done using an Advanced Encryption Standard (AES) key that is generated from a combination of an optional user-supplied password and a key size of 256. After processing all of the Source IPs and User Names in the file, the Collector will output a new “anonymized” version of the input file. Once the Collector has completed outputting the original file as anonymized, compressed, and encrypted sub-files, it will begin to send the files to Cisco using the Secure File Transfer Protocol (SFTP) or HTTPS, depending on user configuration. Once the files have been successfully uploaded, they are deleted from your local machine. Therefore, the customer is required to provide a Server: Physical or Virtual Machine with X86 _64 bit Support with the following characteristics: ■ Processor: 4 Core, Intel(R) Xeon(R) CPU E5-26400 @ 2.50GHz or faster. ■ Memory: 16GB or greater. ■ Hard Disk: 1TB or larger. ■ Operating System: CentOS 6.4/6.5/6.6 X86_ 64 bit –or—Red Hat 6.4/6.5/6.6 X86_64 bit. ■ Operating System Release: 2.6 to 3.0. ■ Operating System Installation Type: Select “Minimal Desktop (Customize later)”. ■ Partitioning: Select “Review and modify partitioning layout.” ❑ /boot: 1 GB (Grub Kernel boot), ext4 file system. ❑ /swap: 16 GB. ❑ /: 817 GB (Rest of the space), ext4 file system. Aside from the Collector software, we require the customer to provide their Internet traffic logs (collected from Web Security gateway, Firewall, SIEM, NetFlow, etc.).The Data Masker is a utility that comes with the Cloud Consumption Collector. The Portal requires Cloud Service Provider (CSP) data from the user’s network for processing, analyzing, and display. This CSP data comes in the form of log files—generated by supported Secure Web Gateways (SWGs), SIEMs, firewalls, Cisco Cloud Web Security (formerly ScanSafe), or NetFlow (v5 and v9). — which then are uploaded to the CC Portal. For

Cisco Cloud Offering	Response
	those users who want to manually upload their log files — they can anonymize log file source IPs and user information (before uploading) with the Data Masker utility.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Cisco Response:

Table 46. New Infrastructure Installation

Cisco Cloud Offering	Response
Metapod	Customer is responsible for the physical installation of new infrastructure (and will have to incur the associated cost). Cisco will be responsible to provision in software configure and provision the infrastructure in the Metapod availability zone.
WebEx	Cisco WebEx manages the Cloud Collaboration infrastructure.
Spark	Customer is responsible for the physical installation of new infrastructure, if required.
Cloud Email Security	Cisco will provide additional infrastructure installation to support business requirements.
Cloud Web Security	Cisco will provide infrastructure installation to support business requirements.
Meraki	The installation of Meraki products often is done by our partner community or customers themselves.
Tropo	Customer shall be solely responsible for, and TROPO is not liable for Customer's failure in, (a) properly configuring, developing, programming, hosting and operating Customer's hardware, software, web sites, Content and all Applications, and their respective telephone and Internet connections, to allow access to and use of the API and Subscriber Services in accordance with the documentation provided by TROPO and all applicable protocols and requirements of the API; (b) thoroughly testing all Applications and related web sites prior to use in connection with the API and the Subscriber Services; (c) ensuring compatibility of the Applications with the API and TROPO's protocols; and (d) providing any connections necessary to communicate with the API.
Cisco Energy Management	Customer is responsible for the physical installation of new infrastructure, if required.
Cloud Consumption as a Service	Customer is responsible for the physical installation of new infrastructure, if required.

8.23 (E) 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).

Cisco Response:

Cisco cloud offerings are aligned with the NIST Cloud Computing Reference Architecture. Per **Figure 3**, Cisco is proposing in our offer cloud services per the Service Layer and per the NIST definitions of IaaS, SaaS, and PaaS. Our cloud offerings are built upon Cisco Validated Architectures that align with the Cloud provider functions as described below and per the NIST Reference Architecture. Our solutions provide the service orchestration, physical and virtual control layers, along with the necessary service management interfaces. Of utmost importance to Cisco is the security and privacy of the infrastructure and its underlying data. As such, Cisco has built application control, policy control, and security analytics into its cloud infrastructure and solutions. This approach involves more than just connecting clouds, but establishing policy across clouds. It ensures network and security policies follow the workload; it harnesses an expanded ecosystem of best-in-class partners and service offerings; it leverages global data while meeting local and regional requirements; and it delivers a unified services catalog, selectively composed of best-in-breed, enterprise-class services and applications. It's about enabling you to build hybrid-ready private clouds, and combining public and private clouds to allow you to enjoy the control, compliance, and security of a private cloud with the flexibility, scalability, and pay-as-you-go benefits of a public cloud.

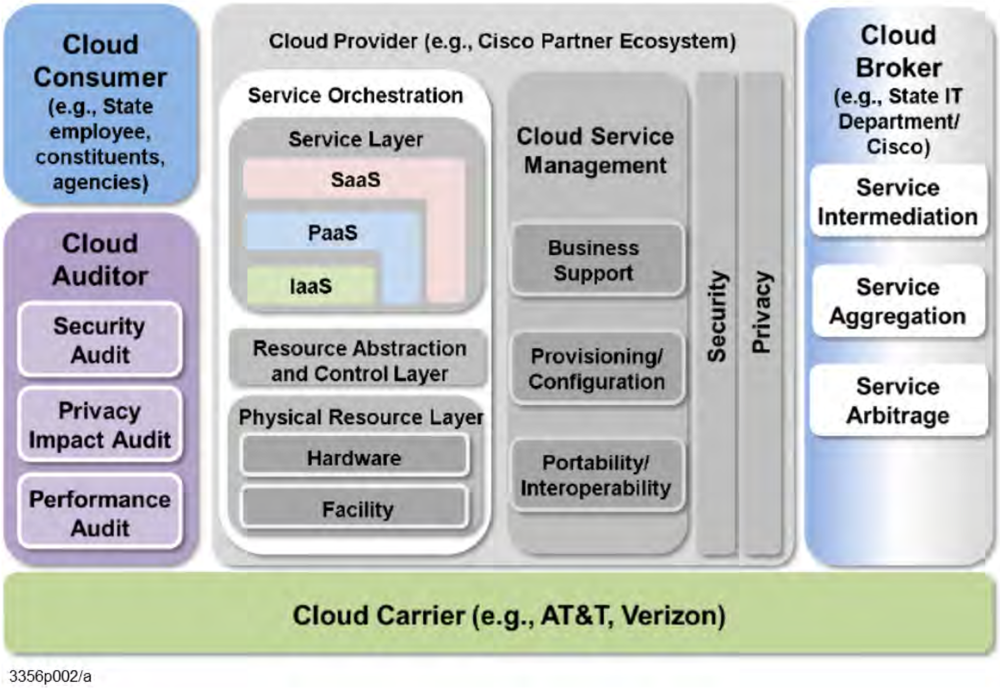

Cloud Consumer (e.g., State employee, constituents, agencies)
Cloud Auditor
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Provider (e.g., Cisco Partner Ecosystem)
Service Orchestration
Service Layer
SaaS
PaaS
IaaS
Resource Abstraction and Control Layer
Physical Resource Layer
Hardware
Facility
Cloud Service Management
Business Support
Provisioning/ Configuration
Portability/ Interoperability
Security
Privacy
Cloud Broker (e.g., State IT Department/ Cisco)
Service Intermediation
Service Aggregation
Service Arbitrage
Cloud Carrier (e.g., AT&T, Verizon)
3356p002/a

Figure 3. Cisco Alignment with NIST Cloud Computing Reference Architecture

Our cloud offerings are designed to help your IT organization act as a service broker to quickly and securely launch and manage new services in any cloud with any VM, and are delivered with a distributed network and security architecture designed for high-value application workloads, real-time analytics, and excellent scalability. Cisco’s Intercloud strategy will empower you to securely use the right cloud for the right service, controlling the right workload with the right policies at the right time.

Confidential, Protected or Proprietary Information

Cisco Response:

Cisco's CAIQ information is proprietary and not publicly available. We request it not be made available for public release.

Exceptions and/or Additions to the Standard Terms and Conditions

Cisco's proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits can be found redlined in:

- Attachment 5 NASPO UT RFP Cloud Services agmt V1 Cisco 030516
- Attachment 6 NASPO UT RFP Cloud Services agmt Exhibit 1 V1 Cisco 022216
- Attachment 7 NASPO UT RFP Cloud Services agmt Exhibit 2 V1 Cisco 022216

Cisco's terms and conditions, license agreements, or service level agreements can be found in:

- Attachment 3 Service Descriptions and SLAs
- Attachment 4 SEULAs

Mimi Nguyen-Farr will be directly involved in contract negotiations and will coordinate with Cisco's legal representatives. She can be reached at:

Name: Mimi Nguyen-Farr

Phone: (408) 527-2627

Email: mimnguye@cisco.com

Cost Proposal

Costing information can be found in:

- Attachment 10 Cisco NASPO Cloud Offerings Price List
- Attachment G — Cost_Proposal.

Attachments

Acronyms

API	Application Programming Interface
ASIG	Advanced Security Initiatives Group
BMS	Building Management Systems
CAIQ	Consensus Assessments Initiative Questionnaire
CCaaS	Cloud Consumption as Service
CC	Contact Center
CEM	Cisco Energy Management
CES	Consulting and Enterprise Solutions
CLI	Command Line Interface
COBC	Code of Business Conduct
CMO	Contracts Management Office
CPU	Computer Processing Unit
CSIRT	Cisco Security Incident Response Team
CWS	Cloud Web Security
D&B	Dun and Bradstreet
DaaS	Desktop as a Service
DDoS	Distributed Denial of Service
DevOps	Development and Operations
DNS	Domain Name System
DRaaS	Disaster Recovery as a Service
FISMA	Federal Information Security Management Act
GCE	Global Compliance Enablement
HCS	Hosted Collaboration Solution
HTTL	High-speed Transistor Translator Logic
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAC	Intelligent Automation for Cloud
IaaS	Infrastructure as a Service
IDC	International Data Corporation
IDS	Intrusion Detection System
IM	Instant Message
IOU	Identify, Observe, and Understand
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NBR	Network Based Recording
NFV	Network Function Virtualization
MX	Mail Exchange
NASPO	National Association of State Procurement
NIST	Network Information Security & Technology
PaaS	Platform as a Service

PCI	Payment Card Industry
PSIRT	Produce Security Incident Response Team
QoS	Quality of Service
R&D	Research and Development
RFP	Request for Proposal
ROS	Remote Operations Services
SaaS	Software as a Service
SHA	Service High Availability
SDN	Software-Defined Networking
SIEMS	Security Incident and Event Management Systems
SKU	Stock Keeping Unit
SLA	Service Level Agreement
SOC	Special Operations Command
TAC	Technical Assistance Center
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPaaS	Telepresence as a Service
UCS	Unified Computing System
VLAN	Virtual Local Area Network
VM	Virtual Machine
WSCA	Western States Contracting Alliance

Attachment E – Contractor's Service Documents
Exhibit A - CLOUD SERVICES

1. **CONTRACTOR CLOUD SERVICES.** The parties agree to the following supplemental terms and conditions, which shall be applicable to the Contractor Cloud Services.

   i. Order Process.

   1. Purchasing Entity will purchase the Contractor Cloud Services, including those made available from Contractor affiliates, which are available on Contractor's Global Price List, through the Purchasing Entity's chosen Fulfillment Partner and the existing order process (i.e., Fulfillment Partner will provide quotes, process Purchase Orders, invoice and collect payment) as set forth in the Contract. The Purchasing Entity and the Fulfillment Partner will also enter into a Statement of Work for the applicable Contractor Cloud Services.

   2. Fulfillment Partners must meet and maintain all required Contractor qualifications and certifications and enroll in the relevant partner programs to sell the applicable Contractor Cloud Services. Contractor reserves the right to review and approve the scope of Purchase Order-based Contractor Cloud Services, and may decline any Purchase Order for Contractor Cloud Services to the extent such Contractor Cloud Services require Contractor to comply with applicable telecommunications statutes, regulations or rules that would require Contractor to obtain additional regulatory filings or applications, make modifications to its pre-existing internal procedures or incur additional expenses in the performance of Contractor Cloud Services under the Contract.

   3. Fulfillment Partners must meet all required Participating State qualifications and certifications and must work with the end Participating Entity to adhere to any required supplemental security policies and procedures.

   ii. **Service Level Availability**. Contractor will maintain availability for the Contractor Cloud Services, excluding connectivity, as set forth in the applicable Documentation or Service Description for such Contractor Cloud Service, and/or agreed in the applicable SLA ("Availability Level"). Any web-based portal as part of the service is not part of the availability SLA.

2. **CMSP SERVICES. T**he following supplemental terms and conditions shall be applicable to the CMSP Services:

   i. **Partner Eligibility.** The CMSP Services are available for purchase from Fulfillment Partners identified as CMSP Partners and approved by the Lead State. Partners must comply with the requirements set forth in this Section, as well as any supplemental terms set forth in an applicable Purchase Order. Partners meeting the Partner eligibility criteria set forth herein are eligible to be added with the Participating State's approval pursuant to the Contract. All partner offerings must include certified Contractor technical support (365X24X7) included as part of the Fulfillment Partner offering.

   ii. **Purchase Order Model.** User Agencies will be able to procure the CMSP Services by entering into a Purchase Order with the Purchasing Entity's selected CMSP partner. The Purchase Order will identify the relevant Cloud-specific payment terms, which for purposes of that particular Purchase Order will supersede any conflicting payment terms in the Contract. The Purchase Order will also set forth relevant business terms and other technical requirements from the Purchasing Entity. For purposes of the purchase and delivery of the CMSP Services, the Purchase Order will provide the Purchasing Entity a direct contractual relationship with the CMSP Partner. The terms and conditions of the Contract shall govern each Purchase Order for purposes of delivery of the services set forth in such Purchase Order.

   iii. **SKUs**. CMSP Services are sold under the applicable Partner's SKU(s). Applicable CMSP Partner SKUs will be provided in a separate tab on the monthly price list update from Contractor for convenience purposes only. Partner SKU(s) will include "CBC" in the pricing column, indicating that pricing will be determined in a Purchase Order on a case by case basis. Contractor disclaims all liability for inaccurate SKUs received from Partners and any other information from

Partners (i.e., CMSP Partner Service Descriptions) related to the CMSP Services subsequently posted on the Contractor pricing website. Purchasing Entities should verify pricing included in Partner quotes and incorporated in the relevant Purchase Order and should not rely on the CMSP Partner information included on the Contractor contract website.

iv. SLAs. CMSP Partners will maintain an Availability Level on the in scope CMSP Services as set forth in the applicable Documentation or Service Description for such CMSP Services, or as otherwise agreed in the applicable SLA. Any web-based portal as part of the service is not part of the availability SLA. Any claims for refunds or other remedies under the applicable SLAs will be solely between the CMSP Partner and the Purchasing Entity. Contractor disclaims all liability for the requirements of the SLAs related to a CMSP Services Purchase Order.

v. Service Descriptions. Each CMSP Partner will have its own service descriptions or program terms (collectively "Service Description") for the approved applicable CMSP Service, which will be incorporated into the Purchase Order. To the extent there is a conflict between the Contract and the CMSP Partner Service Description, the Contract will take precedence. Relevant partner service descriptions will be attached to the applicable quote for CMSP Services. Applicable Service Descriptions will be uploaded on Contractor's contract webpage, which will be updated as additional CMSP offerings become available or additional CMSP Partners are approved to sell under this Agreement. The parties will accordingly amend this Agreement to allow for such additional CMSP offerings. For avoidance of doubt, in the event of a conflict with the version posted on Contractor's website, the Service Description attached to a CMSP Services quote will take precedence over the version posted on Contractor's website. Contractor disclaims all liability for any failure to timely update the CMSP Service Descriptions posted on the Contractor contract website.

vi. **Partner Eligibility.** Partners selling CMSP Services shall have an active "CMSP – Service Provider" certification at all times during the contract term. An Authorized User may terminate a CMSP Purchase Order for breach for a Partner's failure to maintain the required certification(s). To the extent such Purchase Order is terminated for breach under this Section, Contractor will use commercially reasonable efforts to assist the Authorized User in finding another approved CMSP Partner to complete the Term of the CMSP Services.

3. Usage of Purchasing Entity's Sites; Access to Non-Public Systems or Sites

a) To the extent that any Cloud Equipment will be located on Purchasing Entity's Sites, additional terms regarding Cloud Provider's access to such Cloud Equipment, risk of loss related to such Cloud Equipment, and the business continuity plan applicable to such Cloud Equipment will be set forth in a Purchase Order.

b) If, while performing Cloud Services (i) Cloud Provider or any of its agents or subcontractors gains any direct or remote logical access or direct physical access to any Purchasing Entity's computer system (including equipment and software) or any physical access to a non-public part of a Purchasing Entity Site or (ii) Purchasing Entity or any of its agents or subcontractors gains any direct or remote logical access or direct physical access to any Contractor computer system (including equipment and software) or any physical access to a non-public part of a Contractor Site, then:

i. all such access will be strictly limited to that part of the system, Cloud Provider Site or Purchasing Entity Site (as applicable), and will only be carried out in such a manner, as is required for proper performance of the Cloud Services;

ii. each Party will comply with all confidentiality requirements set forth in the Contract, and security procedures and requirements of Cloud Provider or Purchasing Entity pursuant to the Security Appendix to the applicable Purchase Order; and

iii. each Party shall advise the other Party promptly, but in any event at least within ten (10) business days after confirmation that a Security Breach impacted the Cloud Services.

iv. each Party take commercially reasonable measures to address the Security Breach in a timely manner.

4. Security Requirements; Investigations

i. Cloud Provider will comply, and will provide that each of Cloud Provider's Personnel will comply, with:

1. Cloud Provider's internal security standards and Information Security Policies

documented in an applicable Purchase Order or SOW;

2. All applicable site-specific security requirements relating to the Purchasing Entity Sites, as are specified in an applicable Purchase Order or SOW; and
3. Purchasing Entity's internal security standards to the extent that they are applicable to the provision of the Cloud Services and as specified in an applicable Purchase Order or SOW.

ii. In the event the Purchasing Entity's site-specific security policies and/or internal security standards change after the Effective Date of an applicable Purchase Order or Purchasing Entity requests Cloud Provider's compliance with any additional applicable policies provided to Cloud Provider in writing after the Effective Date, the Parties will agree to such compliance pursuant to the Change Request Procedure and to the extent that Cloud Provider can accommodate such request. If Contractor will incur additional costs associated with its compliance with such changes or new policies, the pricing for Cloud Services set forth in the applicable Purchase Order will be adjusted to account for such additional costs, pursuant to the Change Request Procedure. To the extent that such policies conflict with or amend the terms of this Agreement or materially change the Parties' respective risks and liabilities, such policies (or portions of policies) will be followed to the extent they do not conflict with this Section.

iii. Security Investigations, Systems, and Audit

1. The Parties will follow the Security Investigation and Audit obligations and processes set forth in the Contract or an applicable Purchase Order or SOW.
2. Cloud Provider will provide Purchasing Entity with access to Cloud Provider Sites or Cloud Equipment (physical, network, or logical, as specified) only if expressly provided in a Purchase Order. No implied right to access such Cloud Equipment is granted. Any access granted will be subject to the terms of the Agreement and Contractor's Information Security Policies.
3. Purchasing Entity agrees not to perform or allow to be performed any penetration testing, Service performance benchmarking (e.g. application response times, etc.), load testing or similar tests on the Cloud Services unless agreed in writing by Cloud Provider. The Parties agree that the results of any such tests will be Confidential Information and may not be disclosed to Third Parties without advance written permission from Cloud Provider.

5. Acceptable Use Policy: Purchasing Entity agrees to comply with the Cisco Cloud Services Acceptable Use Policy ("AUP") at http://www.cisco.com/c/en/us/about/legal/end-user-license-and-cloud-terms/cloud-services-acceptable-use-policy.html . Contractor may investigate complaints or suspected violations of the AUP and, if Contractor reasonably determines there is a violation, Contractor may take action to remedy the violation (e.g., refusing to post or removing Participating Entity Users' Content or restricting, suspending or terminating access to the SaaS). In instances where Contractor reasonably believes that such violation would expose Contractor to civil, regulatory or criminal liability, Contractor may take action immediately without prior notice to Purchasing Entity. To the extent permitted by applicable law, Purchasing Entity agrees to indemnify, defend and hold Contractor harmless for any claims, liability, damages, and costs (including attorneys' fees) arising from Purchasing Entity's or its Users' violations of the AUP.

6. Use of SaaS/Content: Purchasing Entity owns its Content and is responsible for Purchasing Entity and Purchasing Entity Users' Content and use of the SaaS using Purchasing Entity account information, password, or other login credentials. Purchasing Entity agrees to use reasonable means to protect Purchasing Entity credentials from unauthorized disclosure or use by third parties, and Purchasing Entity will promptly notify Contractor of any unauthorized use of Purchasing Entity account of which Purchasing Entity becomes aware. Any registration information Purchasing Entity provides to use the SaaS will be accurate and Purchasing Entity will keep such information current and up to date. Purchasing Entity will not sell, resell, reframe, distribute, rent or lease the SaaS, include the SaaS in an outsourced or service bureau offering, or otherwise commercialize the SaaS. Purchasing Entity grants Contractor a worldwide, royalty-free, sublicensable license to use, modify, reproduce and distribute the Content only as reasonably required to provide the SaaS. Contractor is free to use and incorporate any feedback Purchasing Entity provides regarding the SaaS without payment of royalties or other consideration.

COMMENT:
The following is a sample Statement of Work (SOW). Depending on the particular service offering which is offered by a Contractor under the Master Agreement and selected by a Purchasing Entity and agreed by the parties in an applicable SOW, certain exhibits may be added to include SOW, SOW format, transition services, change management, and other elements of the cloud services offering.

[SAMPLE]

CLOUD SERVICES STATEMENT OF WORK
[PROJECT NAME]

This Statement of Work ("SOW") for Cloud Services is entered into between [Cloud Provider full name], a [state of incorporation] corporation having a principal place of business at [address] (["Fulfillment Partner"/ "Cloud Provider"]), and [Purchasing Entity], a [public sector agency/higher educational institution/etc.] having a place of business in ____ at [customer address] ("Customer"), and is entered into as of the date of signature as last written below ("SOW Effective Date").

For convenience, the parties agree this SOW is governed by the Participating Addendum, effective________________, as amended, between Contractor and Participating Entity ("Contract") with Contractor Reference __________________ [if CMSP Services SOW, add: However, Customer agrees that Contractor is not a party to this SOW and has no liability for the Fulfillment Partner's compliance with the terms or performance of the Cloud Services under this SOW.] The terms of this SOW are limited to the scope of this SOW, and shall not be applicable to any other Statements of Work executed between the parties. Capitalized terms used in this SOW and not otherwise defined shall have the meanings given them in the Contract. To the extent there is a conflict between the terms of this SOW and the Contract, the terms of the SOW shall control with respect to the subject matter of the SOW, unless explicitly stated otherwise in this SOW.

This SOW consists of this signature page and the following sections:

Exhibit 1: Project Scope, Responsibilities and Pricing

Exhibit 2: SOW Process, and Terms & Conditions

Appendix A: Example Milestone Completion Certificate **[Delete if not applicable]**

Appendix B: Example Change Request for SOW-based Cloud Services

AGREED:

Each party, as evidenced by the signature below or electronic signature, as applicable, of its authorized representative, acknowledges that it has read and agrees to this SOW in its entirety.

[Cloud Provider **Full Legal Name]**

By: ______________________________

Name: ______________________________

Title: ______________________________

Date ______________________________

[Customer Full Legal Name]

By: ______________________________

Name: ______________________________

Title ______________________________

Date ______________________________

[SAMPLE]

CLOUD SERVICES STATEMENT OF WORK
EXHIBIT 1 – PROJECT SCOPE, RESPONSIBILITIES, AND PRICING

1.0 PROJECT SCOPE

Project Name: [Project Name]

End User

Cloud Provider shall provide the following Cloud Services and Deliverables to [Customer name] ("End User") or ("Customer").

1.1 Services

As more fully described in Section 2.0 – "Responsibilities of the Parties", Cloud Provider shall provide the following Cloud Services to End User, during Standard Business Hours, unless explicitly stated otherwise in this SOW.

- **[SKU Reference and SKU description]**

1.2 Scope of Cloud Services

[Type of Cloud Services]
<<Remove this section if there is no Services Summary to include. Please ensure that if you insert a Services Summary, it should only be a high level and necessary description of the services to be provided. This summary is not intended to replace any other section of the SOW>>

1.3 Document Deliverables

As more fully described in Exhibit 2, Section 3.0, Cloud Provider shall provide for review and approval the following Document Deliverables:

- **[Describe, if any or state "None"]**

1.4 Location of Services

Services shall be performed as a combination of remote from Cloud Provider Site(s) and onsite at the following End User (or Integrator) Site(s):

- [Insert location]

1.5 Product Summary

[The Cloud Services performed in accordance with this SOW apply to the Products listed below **OR** in Appendix C: Bill of Materials (BOM). **OR** This SOW does not apply to the purchase of the Products.]

1.6 Services Schedule

The following is the initial schedule of Services:

Service Name/Project Task	Targeted Commencement Date (Business Days)	Targeted Completion Date in Elapsed Time (Business Days)

[Name of Services] (Remote and On Site)	T0	T0 + 90 Business Days

Services shall not commence until this SOW has been fully executed, Cloud Provider has accepted a valid Purchase Order, and has scheduled the start of Services (“Start Date”) or (“T0”).

Cloud Provider has a lead time of [Forty-Five (45)] Business Days to schedule the start of Cloud Services. Cloud Provider will notify Customer in writing of the actual commencement date of Cloud Services.

All changes affecting the baseline schedule are subject to agreement by Customer and Cloud Provider and managed through the Change Management Procedures as specified herein.

The final Cloud Services Schedule shall be mutually determined by Cloud Provider and the Customer, and documented in writing.

1.7 Single Point-of-Contact Information

Customer and Cloud Provider shall designate a single point of contact to whom communications in regards to the Cloud Services may be addressed and who has the authority to act on all aspects of the Cloud Services; shall be available during Standard Business Hours; and shall designate a backup contact for when the primary contact is not available.

Cloud Provider Contact Name:		**Customer Contact Name:**	**{. . .}**
Title:		Title:	{. . .}
Telephone Number:		Telephone Number:	{. . .}
E-mail Address:		E-mail address:	{. . .}

2.0 RESPONSIBILITIES OF THE PARTIES

2.1 [Insert Cloud Provider and Customer Responsibilities based on the type of Cloud Services]

Cloud Provider Responsibilities:

Customer Responsibilities:

General Customer Responsibilities: [Revise/Delete as relevant to the Cloud Services]

i. Designate a single point of contact to act as the primary technical interface to the designated Cloud Provider engineer.

ii. Ensure key Customer personnel (such as: architecture design and planning, network engineering, network operations staff) are available to participate during the course of the Service (to provide information and to participate in review sessions).

iii. Provide documented Customer requirements (business and technical) and high-level network architecture design specifications.

iv. Provide documented information on Customer's existing network infrastructure design including such as: features and services, route plans, addressing schema, call/data flow, dial plans, security policies, network management and operational processes.

v. Unless otherwise agreed to by the parties, Customer shall respond within five (5) Business Days of Cloud Provider’s request for any other documentation or information needed to provide the Cloud Service.

vi. Customer agrees to utilize Collaboration Tools.

vii. The following is required for Customer’s use of Collaboration Tools: a). Customer will provide the names and other pertinent information (such as e-mail account information) of Customer resources who require authorization to access; b). Customer will support the implementation of software required to use the Collaboration Tools in their environment; c). Customer will download Collaboration Tools guest client(s), if applicable, if not already in possession of the applicable license; and d). Customer agrees to immediately return Collaboration Tool(s) to Cloud Provider, as instructed by Cloud Provider, upon the earlier of: (i) completion of Services; or (ii) Cloud Provider’s request to Customer that the Collaboration Tool(s) be returned to Contractor.

3.0 ASSUMPTIONS

Services and service pricing are based upon the following assumptions and exclusions (“Assumptions”). Any additional costs identified as a result of deviations from these Assumptions will be managed through the Change Management Procedures specified in this SOW. Customer and Cloud Provider agree that any changes in the Assumptions may result in an adjustment in the pricing stated in this SOW.

a. This SOW should be read in conjunction with the SOW General Assumptions and Exclusions document posted at: www.cisco.com/go/servicedescriptions which is hereby incorporated into this SOW by this reference. To the extent there is a conflict between the terms of this SOW and such document, the terms of this SOW shall control.

b. Customer is responsible for determination of its design requirements and the utilization of any recommendations provided by Cloud Provider. Cloud Provider recommendations are based upon Customer information provided by Customer at the time of the services. Cloud Provider shall not be liable for the accuracy or completeness of the Customer provided information contained in the Cloud Provider recommendations.

c. Each party acknowledges that completion of Services by the Targeted Completion Date is dependent upon the other party (each as appropriate and as further described in Section 2.0 above) meeting its obligations in this SOW.

[insert any additional assumptions that are project specific.]

4.0 PRICING

4.1 Pricing Table

Customer will issue Purchase Orders in accordance with the following Cloud Services Pricing scenario.

Services Part Code	Term (months)	Service Description	Unit Price (USD)	Extended Price (USD)
			$INSERT	$INSERT
			Total Price:	$INSERT

Pricing premised upon Cloud Services provided by non-union labor.

4.2 Travel and Expense

Travel and Expense (“T&E”) is/is not included, or itemized in the above pricing. [Pricing is for Remote Services only or End User Site is considered to be local and Travel and Expense (T&E) is not necessary. OR To the extent T&E is included, such expenses will be governed by Purchasing State’s Travel Policy.

4.3 [Milestone] Invoice Schedule [if billed on a Milestone Basis]

Cloud Services will be invoiced upon completion of each Milestone as set forth in the following Milestone Invoice Schedule (MIS) and in accordance with Exhibit 2, Section 4 “Completion”:

Milestone #	Milestone Description	Invoice Amount (USD)
1.		$INSERT
	Total:	**$INSERT**

This MIS supersedes any Milestones identified in a Purchase Order; provided however, the total invoiced amounts for Milestones will not exceed the total amount of Integrator's Purchase Order unless such amounts are mutually agreed upon pursuant to the Change Management Process under Exhibit 2.

Any changes to the MIS will be managed through the Change Management Procedures specified in Exhibit 2 of this SOW.

SAMPLE

CLOUD SERVICES STATEMENT OF WORK
EXHIBIT 2 – SOW PROCESS AND TERMS AND CONDITIONS

1.0 ORDERING AND COMMENCEMENT

1.1 Prior to Cloud Provider performing the Services, Customer must have:

i. A fully executed SOW, and

ii. Issued a valid Purchase Order to Cloud Provider for the Cloud Services.

1.2 The term of each SOW commences on the SOW Effective Date and shall continue until [last Milestone completion or Termination Date].

1.3 The SOW shall be governed by the terms and conditions of the Participating Addendum (the “Contract”) executed by Cisco Systems, Inc. and the ____ (“Customer”) and shall be interpreted based on the order of precedence set forth in the Contract, as amended. For purposes of delivery of the services set forth in this SOW, the Cloud Provider will be responsible for all legal obligations of the Contract as if such Cloud Provider were the prime contractor. This SOW shall create a direct contractual relationship between the Cloud Provider and the Customer.

2.0 PURCHASE ORDER

Purchase Orders shall be issued to the Fulfillment Partner and sent to the following:

Cloud Provider Services Manager:	Services Account Manager	Email Address:	Email address

2.1 Purchase Order Issuance:

2.1.1 Customer shall purchase Cloud Services by issuing a Purchase Order to the Cloud Provider, subject to Cloud Provider’s acceptance and Contractor’s approval of the scope, for the total price identified herein. Each Purchase Order must be signed, if requested by Cloud Provider, or (in the case of electronic transmission) sent, by an authorized representative and indicate the following information:

a. SOW/Project ID Number;

b. Travel and Expense Part No., Price, (if applicable as a separate line item);

c. Total Purchase Price;

d. Bill-to, and Ship-to (Service-to) addresses;

e. Requested Services Start Date; and

2.1.2 All Purchase Orders issued for the Cloud Services identified in this SOW must reference this SOW as well as the Contract number. The terms and conditions of this SOW prevail regardless of any conflicting terms on the Purchase Order, other correspondence and any and all verbal communications.

2.2 Term. The SOW Term shall be from the date of last signature below (“Effective Date”) and shall continue until ____ [SELECT 1, 3 or 5 year term based on offering] unless terminated earlier in accordance with the terms of the Contract or this SOW.

2.3 The terms of this SOW including the pricing set forth herein are valid only for a period of sixty (60) calendar days from date of submittal unless fully executed within such period.

2.4 Date of Submittal: [date]

2.5 [Insert details] Services Part No., Quantity, Price, Billing Model (i.e., flat fee, milestone-based, usage based, overage calculations, if any), Payment Due Date(s).

3.0 DOCUMENT DELIVERABLE REVIEW AND APPROVAL PROCESS [IF APPLICABLE – DELETE IF NO DOCUMENT DELIVERABLES]

For Document Deliverables that are subject to review and approval from Customer, the parties will adhere to the following review and approval process:

3.1 Cloud Provider will present the draft Document Deliverable to Customer when the document is ready for review and approval.
3.2 Customer shall review the draft Document Deliverable with Cloud Provider, providing written comment or approval of the Document Deliverable within five (5) Business Days immediately after completion of such review.
3.3 If no written (including email) comment or approval is received by Cloud Provider within said time period, the Document Deliverable as provided by Cloud Provider is deemed to be accepted by the Customer.
3.4 If Customer provides comments, then Cloud Provider shall address such comments in a timely manner and this process for review and approval will be repeated.
3.5 No further Cloud Services as defined in the SOW will be performed until the Customer's acceptance of Document Deliverables is received by Cloud Provider.

4.0 COMPLETION [ONLY APPLICABLE TO MILESTONE BASED SOWS]

Customer's review and approval of all milestones provided to Customer will adhere to the following process:

4.1 Cloud Provider shall notify Customer of Cloud Provider's completion of a Milestone or Service by submitting to Customer a Milestone Completion Certificate ("MCC") (an example of which is provided as Appendix 4A).
4.2 Customer has ten (10) Business Days from the receipt of the MCC to sign and return the MCC to Cloud Provider.
4.3 Customer's signing of the MCC, or Customer's failure to respond to the MCC within the ten (10) Business Day period, signifies Customer's acceptance that Cloud Provider has performed the Cloud Services listed in the MCC in accordance with the SOW.
4.4 To decline acceptance of the MCC, Customer must provide to Cloud Provider in writing that the MCC has been declined, and detail how the Cloud Services have not been performed by Contractor in accordance this SOW.
4.5 Cloud Provider shall address any such non-conformance in a timely manner. Cloud Provider shall compile an action plan to correct any non-conformance and the process for acceptance detailed herein will be repeated until such time as all non-conformances have been resolved. Acceptance may not be declined due to defects in Services that do not represent a material non-conformance with the requirements of this SOW. Any dispute regarding whether a non-conformance is material will be addressed in accordance with Section L.8 (Dispute Resolution) of the Contract.
4.6 Customer shall not delegate or assign the task of accepting or assessing completion of Milestones.

5.0 CHANGE MANAGEMENT PROCEDURES

5.1 It may become necessary to amend this SOW for reasons including, but not limited to, the following:
5.1.1 Changes to the scope of work and/or specifications for the Services,
5.1.2 Changes to the Milestone Invoice Schedule (MIS), [if applicable]
5.1.3 Changes to the project schedule,
5.1.4 Unavailability of resources which are beyond either party's control, and/or,
5.1.5 Environmental or architectural conditions not previously identified.

5.2 A request for a change may be initiated by either party in accordance with the procedure outlined below:
5.2.1 The party requesting the change will deliver a "Change Request" to the other party (an example of which is provided in Appendix B). The Change Request will describe the nature of the change, the reason for the change and details of the likely impact, if any, on the project's schedule, scope, pricing and payment.
5.2.2 The parties will evaluate the Change Request and negotiate in good faith the changes to the Services and additional fees, if any, required to implement the Change Request. If both parties

agree to implement the Change Request, both parties will sign the Change Request, indicating the acceptance of the changes by the parties.

5.2.3 Upon execution of the Change Request, the Change Request will be considered an amendment of this SOW.

5.2.4 Cloud Provider is under no obligation to proceed with the Change Request until both parties agree to and sign the Change Request.

5.3 Whenever there is a conflict between a fully executed Change Request and the original SOW, or a previous fully executed Change Request, the terms and conditions of the most recent fully executed Change Request will prevail.

6.0 SERVICE DESCRIPTION. The applicable Service Description for the Cloud Services is attached at Appendix __ hereto.

7.0 SERVICE LEVEL AGREEMENT. [Cloud Provider will provide a minimum Service Level as set forth in the applicable Documentation or Service Description for the applicable Service offering.] Insert SLA here ___________________.

8.0 SUPPLEMENTAL DATA SECURITY OBLIGATIONS [IF APPLICABLE MAY BE NEGOTIATED WITH CLOUD PROVIDER AND CUSTOMER]

8.1 Order of Precedence. In the event that any of the terms of the security policies conflict with one another, with regard to the provision of the Cloud Services, "Cloud Provider's obligation to comply with the conflicting policies will be based on the following order: (i) first, Cloud Provider's security policies, (ii) second, Purchasing Entity's internal security standards, and (iii) and third, Purchasing Entity's site-specific requirements, as applicable. [ORDER MAY BE REVISED BASED ON CUSTOMER'S REQUIREMENTS. ANY CHANGE FROM ORDER OF PRECEDENCE SHALL BE DOCUMENTED IN A MUTUALLY AGREED UPON SOW]

8.2 **[Insert customers specific technical security requirements, certifications or third party audit here]**

8.2.1 All non-public data shall be owned by Customer.

8.2.2 Cloud Provider will not use Customer Data for any purpose that is not customer-related.

8.2.3 [Identify Customer access and import/export rights for Customer Data.]

8.2.4 Cloud Provider will notify Customer in the event of E-discovery, a litigation hold, discovery search, or request for access by law enforcement or courts for the above requests. [specify how notification will take place and processes to follow-up on such requests]

8.2.5 Servicing Open Records [if Cloud Provider will host data that is subject to disclosure under open records];

8.2.6 Records Retention for the statutory period – if applicable (i.e., tax records, tax advise)

8.2.7 Advance notice of major upgrades, system changes and maintenance [include in SOW if not already set forth in a Service Description]

8.2.8 Timing notice regarding scheduled outages and data recovery [include in SOW if not already set forth in a Service Description]

8.2.9 [Background checks – identify requirements]

8.2.10 [etc]

8.3 **Encryption at Rest.** Encryption at rest requirement may be deleted from this Section based on the required functionality of the service offering and Cloud Provider and Customer shall use commercially available encryption technologies that conform to applicable laws and regulations. Approved encryption methods are limited to those algorithms that have received substantial public review and have been proven effective.

8.4 **Physical and Environmental Security of Data Center(s).** Based on FIPS 199, Customer will determine data, information, and information system categorization. If categorization level is moderate or higher, any physical data center security requirement shall be mutually agreed upon and documented in the SOW.

8.5 **[audit requirements]**

8.6 **[compliance with other requirements]**

9.0 ADDITIONAL TERMS AND CONDITIONS

9.1 FULFILLMENT PARTNER CERTIFICATIONS

9.1.1 Fulfillment Partner confirms is has the appropriate certifications required to sell the Cloud Services ordered hereunder, including the following:

[insert list of relevant Fulfillment Partner certifications]

9.1.2 [IF CMSP SERVICES] Fulfillment Partner confirms it is using the Contractor-powered infrastructure and Contractor-validated solution designs in providing the Cloud Services ordered hereunder.

9.2 Technical Requirements **[IF APPLICABLE MAY BE NEGOTIATED WITH CLOUD PROVIDER AND CUSTOMER]**

9.2.1 [insert here: e.g., web-based, SLA Mgt, rapid provisioning, API restful, monitoring and reporting]

9.2.2 Data Portability [insert if applicable]

9.2.3 Workload Portability [insert if applicable]

9.2.4 Monitoring [insert if applicable]

9.2.5 Security Infrastructure [insert if applicable]

9.2.6 Disaster Recovery/Business continuity [insert if applicable]

9.2.7 Data preservation

9.2.7.1 Cloud Provider agrees to store data past termination for [30/60/90, etc.] days in accordance with the terms set forth in Section _, Exit Assistance.

9.2.7.2 [Secure data deletion]

9.3 Support

9.3.1 Fulfillment Partner will engage Contractor to provide 7x24 technical support services on the back end for the Cloud Services.

9.3.2 Fulfillment Partner will utilize an online portal for a trouble ticket system to track technical support issues.

9.3.3 Fulfillment Partner will provide “follow-the-sun” model for maintenance and support.

9.3.4 [Scheduled Outage and Maintenance Reporting]

9.4 [additional terms to be negotiated as appropriate for the type of Cloud Services offered]

[ONLY APPLICABLE FOR MILESTONE BASED CLOUD SERVICES
DELETE IF SOW IS FOR SUBSCRIPTION BASED CLOUD SERVICES]
Please note that this MCC is provided as an example and should not be filled in until relevant services are complete.

SAMPLE

CLOUD SERVICES STATEMENT OF WORK
APPENDIX A: EXAMPLE MILESTONE COMPLETION CERTIFICATE (MCC)

Pursuant to the Statement of Work ("SOW") referenced as Project ID Number: [project ID] between [Cloud Provider name] ("Cloud Provider") and [Customer Name] ("Customer"), Customer hereby certifies, by the signature below or electronic signature, as applicable, of its authorized representative, that the Service Milestone described below has been completed on the date indicated below and in accordance with the terms of the SOW.

Milestone #	Milestone Description	Milestone Completion Date	Invoice Amount {. . .}
1.	Completion of		
	Total:		$

Customer Purchase Order Number	Cloud Provider Sales Order Number	Contractor Part Number	Invoice Amount {. . .}
<Enter PO# Here>	<Enter SO# Here>	<Enter Product Code>	$
<Enter PO#>	<Enter SO# Here>	Travel and Expense (T&E) BS-TEBILLINGS	$

Total Invoice Amount of Services Completed: $

Is this the last Milestone Completion Certificate? (Yes/No): YES/NO

End User:

Integrator has five (5) Business Days from the receipt of this MCC to sign and return this MCC to Cloud Provider.

Integrator's signing of this MCC, or Integrator's failure to return this MCC within five (5) Business Days, signifies Integrator's acceptance that Services listed above have been performed according to the S

Submitted By:

[Cloud Provider]

MCC Submittal Date: ______________________

Acknowledged and Agreed:

[Customer Name]

By: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

EXHIBIT 2

END USER LICENSE AGREEMENT

[Attach applicable SEULAs]

1. **End User License Agreement**. Contractor or its affiliate licensing the Software is willing to license this Software to Customer (Customer as referred to herein shall mean State, or a Purchasing Entity, as applicable, for the entity ordering the Software) only upon the condition that Customer purchased the Software from an approved source and that Customer accepts all of the terms contained in this end-user license agreement plus any additional limitations on the license set forth in a supplemental license agreements ("SEULAs") which are attached to and incorporated and made a part of this End User License Agreement, or are later incorporated by amendment to be made a part of this Agreement (collectively, the "agreement"). To the extent of any conflict between the terms of this end EULA and any SEULA, the SEULA shall apply. By downloading, installing, or using the Software, Customer represents that it has purchased the Software from an approved source and binds itself to the agreement. If Customer does not agree to all of the terms of the agreement, then Contractor is unwilling to license the Software to Customer and (a) Customer may not download, install, or use the Software, and (b) Customer may return the Software (including any unopened cd package and any written materials) for a full refund, or (c), if the Software and written materials are supplied as part of another product, Customer may return the entire product for a full refund. Customer's right to return and refund expires 30 days after purchase from an approved source, and applies only if Customer is the original and registered end user purchaser. For the purposes of this end-user license agreement, an "approved source" means (a) Contractor; or (b) a distributor or systems integrator authorized by Contractor to distribute/sell Contractor equipment, Software, and services within your territory to end users; or (c) a Fulfilment Partner authorized by any such distributor or systems integrator in accordance with the terms of the distributor's agreement with Contractor to distribute/sell the Contractor equipment Software and services within your territory to end users.

2. **Terms of License.** Conditioned upon compliance with the terms and conditions of the license granted herein or as represented in the applicable Contractor's End User License Agreement, Contractor grants to Customer a nonexclusive and non-transferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees, subject to the terms herein.

   a. Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or that number of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s), or site(s), as set forth in the applicable Purchase Order which has been accepted by Contractor and for which Customer has paid to Contractor the required license fee.

   b. Unless otherwise expressly provided in the documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Contractor equipment) for communication with Contractor equipment owned or leased by Customer and used for Customer's internal business purposes. For evaluation or beta copies for which Contractor does not charge a license fee, the above requirement to pay license fees does not apply.

3. **General Limitations**. This is a license, not a transfer of title, to the Software and Documentation, and Contractor retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Contractor, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

   i. transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or second-hand Contractor equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense, or use shall be void;

ii. except as approved in writing by Contractor, make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

iii. reverse engineer or decompile, decrypt, disassemble, or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

iv. use or permit the Software (other than embedded in the product) to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Contractor; or

v. except and to the extent expressly required by a Purchasing State's applicable records laws or final court order (provided that the Purchasing State provides: (1) prior written notice to Contractor of such obligation and (2) the opportunity to oppose such disclosure, provision, or otherwise making available), disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Contractor. Customer shall implement reasonable security measures to protect such trade secrets.

4. To the extent required by law, and at Customer's written request, Contractor shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Contractor's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Contractor makes such information available.

5. **Software, upgrades/updates, and additional copies.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS MASTER AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CONTRACTOR EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

6. **Proprietary Notices.** Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Contractor.

7. **Term and Termination of License**. This license granted herein shall remain effective until terminated. Customer may terminate the license at any time by destroying all copies of Software and any Documentation except as to the minimum number of copies required by law to keep for archival records purposes only. Customer's rights under this license will terminate immediately if Customer fails to comply with any material provision of this license and Contractor will give Customer notice of such non-compliance. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control.

8. **Customer Records**. As permitted by applicable law, Customer grants to Contractor and its independent accountants the right to examine Customer's books, records, and accounts during Customer's normal business hours to verify compliance with this license. In the event such audit discloses non-compliance with this license, Customer shall promptly pay to Contractor the appropriate license fees, plus the reasonable cost of conducting the audit. In all other circumstances, the audit fees shall be paid by Contractor.

9. **Warranty.**

i. Hardware. Contractor warrants that from the date of shipment by Contractor to Customer, and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the Warranty Card accompanying the product, the Hardware will be free from defects in material and workmanship, under normal use. This limited warranty extends only to the original user of the product. Customer's sole and exclusive remedy and the entire liability of Contractor and its suppliers under this limited warranty will be, at Contractor's or its service center's option, shipment of a replacement within the period and according to the replacement process described in the Warranty Card, freight and insurance prepaid, or if the Hardware is a necessary and dependent part of a Service provided by Cisco, Customer’s sole and exclusive remedy will be the refund of amounts already paid by Customer for such Services, but that Customer is unable to use, due to the defect.. Contractor replacement parts, used in Hardware repair, may be new or equivalent to new. Contractor’s obligations hereunder are conditioned upon the return of affected products, in accordance with Contractor’s then-current Return Material Authorization (RMA) procedures.

ii. Software. Contractor warrants that from the date of delivery by Contractor to Customer (but in case of resale by a Contractor Fulfilment Partner, commencing not more than ninety (90) days after original shipment by Contractor), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the Warranty Card accompanying the product (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship, under normal use; and (b) the Software substantially conforms to its published specifications. The date of shipment of a product by Contractor is set forth on the packaging material in which the product is shipped. In no event does Contractor warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Contractor does not warrant that the Software or any equipment, system, or network on which the Software is used will be free of vulnerability to intrusion or attack. Notwithstanding the foregoing, Contractor warrants that the Software, when shipped by Cisco or when made available for download from CCO, is free from Viruses. As used herein, the term "Viruses" means codes, programs or commands designed to (1) alter, damage or erase computer data or programs or (2) permit unauthorized access to Customer systems, any of which is intended to destroy or cause the Customer's system to malfunction. Customer’s sole and exclusive remedy and the entire liability of Contractor and its suppliers under this limited warranty will be, at Contractor or its service center’s option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer, if different than Contractor. If the Software is a necessary and dependent part of a Service provided by Cisco, Customer’s sole and exclusive remedy will be the refund of amounts already paid by Customer for such Services, but that Customer is unable to use, due to the Software Virus. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee.

iii. Restrictions. This warranty does not apply if the product (a) has been altered, except by Contractor, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Contractor, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is sold or, in the case of Software, licensed, for beta, evaluation, testing, or demonstration purposes for which Contractor does not receive a payment of purchase price or license fee.

The above warranty does not apply to any beta software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which Contractor does not receive a license fee. All such software is provided AS IS without any warranty whatsoever.

Software and related documentation are “commercial items” as defined at Federal Acquisition Regulation (“FAR”) (48 C.F.R.) 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in FAR 12.212.

Cisco WebEx LLC
Service Level Addendum

This Service Level Addendum for the WebEx Service ("SLA") is intended to provide special terms and conditions that govern an availability service level commitment in connection with a purchase of WebEx Web Based Application Services (the "Services"). "Services" shall mean only those WebEx Services designated on an Order Form, purchase order or other ordering tool that has been issued by the purchaser and accepted by the Service provider. Services, as defined herein, are exclusive of Cisco and Iron Port products and services.

Direct Sale from WebEx or Cisco. If the Services are being purchased directly from Cisco or WebEx, this document is incorporated into the Cisco WebEx Software as a Service Agreement or equivalent services agreement ("SaaS") executed between you, the purchaser, and Cisco Systems, Inc. (or its affiliate) (in any case, "Cisco") or Cisco WebEx LLC (or its affiliate) (in any case, "WebEx"). In the event of a conflict between the SaaS and this SLA, this SLA shall prevail.

Sales via WebEx Reseller. If the Services are being purchased by a WebEx reseller, this document is incorporated into the WebEx Services Resale Agreement or equivalent resale agreement ("GRA"), executed by you, the reseller, and WebEx, and is conditional upon you, the reseller, entering into a substantially similar service level agreement your customer. In the event of a conflict between the GRA and this SLA, this SLA shall prevail.

Sales via Cisco Authorized Reseller. If the Services are being purchased through a "Cisco Authorized" Reseller, this document is incorporated into the Systems Integrator Agreement, Special Purpose Systems Integrator Agreement for Collaboration Technology or Indirect Channel Reseller Agreement or equivalent partner agreement ("SIA") (and the applicable Service Description) executed by you, the reseller, and Cisco, and is conditional upon you, the reseller, entering into a substantially similar service level agreement your customer. In the event of a conflict between the SIA and this SLA, this SLA shall prevail.

Availability Level. WebEx will maintain 99.5% availability of its Web Based Application Services (including telephony services) to the Internet (excluding scheduled maintenance intervals) ("Availability Level").

Down Time Credit. For any cumulative time periods in excess of that contemplated by Availability Level for which the Services are unexpectedly unavailable to the Internet ("Down Time"), WebEx or Cisco (in either case, the "Company") will credit the customer (if the purchase is made directly) or reseller (if the purchase is made indirectly) the amount of Subscription Service Fees or License Fees, as applicable, owed in an amount equal to that portion of the month attributable to the Down Time; provided that (i) use of the Services is impacted, (ii) the Down Time is reported within twenty four (24) hours of each occurrence, and (iii) the party purchasing from the Company, as applicable, requests credits not more than thirty (30) days after each occurrence. The terms and conditions of this section shall be the purchaser's sole and exclusive remedy and the Company's sole obligation for any Down Time.

Confidentiality. All parties agree that the existence and terms of this SLA and the issuance of any credits in accordance with this SLA, are strictly confidential and shall only be disclosed to the customer or reseller, and to employees of the parties on a "need to know" basis for purposes of fulfilling the parties' obligations hereunder. Neither party will disclose to any third party (other than a purchasing customer) the existence, intent, or terms of this SLA without the prior written consent of the other party

Credit Availability. If Services are prepaid, a Credit Memo will be issued. The Credit Memos described above may be applied by the party purchasing from the Company toward the purchase of Company products or services (for any end-customer) during the 12 months following issuance of such credits. Any credit not used within such 12 month period shall be void and have no value. Credits may not be converted to refunds, used as set off from any amount owing to Cisco or WebEx, nor transferred or assigned.

.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

END USER LICENSE AGREEMENT FOR THE TIDAL SOFTWARE PRODUCTS

Software
For purposes of this Supplement, the Software covered under this SEULA includes the following and each of their respective associated components and modules:

Tidal Enterprise Scheduler
Cisco Process Orchestrator
Tidal Performance Analyzer
Cisco Intelligent Automation for Compute
Cisco Intelligent Automation for Cloud
Cisco Intelligent Automation For Cloud Starter Edition
Cisco Server Provisioner
Cisco Intelligent Automation for SAP

Definitions

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

For purposes of this Supplement, the following defined terms will apply:

Designated System shall mean the designated platform for which Customer originally licenses the Software from Cisco for installation and use. Such designated platform may include for instance, but is not limited to, a designation of the specific number of CPUs or system description or name as approved by Cisco.

Movement and Usage Fees shall mean fees applicable as set solely by Cisco for the transfer and installation of Software on a system that is not a Designated System.

Total Deployment Size shall mean the designated configuration for which the Cisco Intelligent Automation For Cloud Starter Edition Solution cannot exceed 160 blades collectively across a customer s installation.

Other Terms and Conditions

Movement and Usage. With respect to the license granted to Customer in the Agreement, such license is applicable only to the Designated System. Movement of Software to another system requires Customer providing prior written notice to obtain updated keys, and additional fees may apply. A fee schedule is available upon Customer s written request to Cisco.

License. For the avoidance of doubt, the license granted to the Software in the license section shall be perpetual if designated as such by Cisco at time of Customer order for the Designated System, subject to payment of any applicable fees, including, but not limited to, any Movement and Usage fees described above.

Total Deployment Size. For avoidance of doubt, no customer shall deploy the Cisco Intelligent Automation For Cloud Starter Edition Solution in a configuration that exceeds 160 blades in total deployment size across their enterprise.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

If you have licensed Cisco Workplace Portal, the following additional terms apply:
Cisco Workplace Portal is licensed for use with end user and workplace-related services including non-server computers, computer accessories, PDAs and handhelds, desktop software, mobility, unified communications, end user applications, email management, access to printing or files, office and wireless phones, voicemail, calling cards, video conferencing facilities and other workplace-related services for the greater employee base.
Cisco Service Connectors and Adapters are not for use with the Cisco Workplace Portal.
If you have licensed Cisco Cloud Portal, the following additional terms apply:
Cisco Cloud Portal is licensed for use with cloud computing and data center-related services including compute, storage, network, IaaS, PaaS, application hosting, database services, application development & maintenance, application installations & upgrades, dedicated application hosting, disaster recovery, network administration, application testing, and systems monitoring.

Cisco Cloud Portal is licensed for use only in the management of service catalogues and provisioning of computing and SW components that relate to a cloud computing and orchestration infrastructure maintained and managed by the licensee.

Cisco Service Connector is licensed for the following functions: Core Functions Adapter, Windows Adapter (a single instance for the Windows server hosting the Cisco Process Orchestrator (CPO) Engine), email adapter, single instance of Active Directory (AD)

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Adapter (a single instance for the domain in which the server is installed), Core Automation Pack, Common Activities Automation Pack, and the Tasks Automation Pack.
CPO elements included in Cisco Service Connector can only be used with licensed components listed below:
Cisco Service Connector Web Service Adapter -- Limited to 5 connections to Web Services for newScale Request Center for Cloud and third-party Orchestrators.
Cisco Service Connector Terminal Adapter -- Limited to 1 terminal or UNIX/Linux target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector VMware Adapter -- Limited to 5 connections to VMware vCenter for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Microsoft Community Adapter -- Limited to 1 Windows target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Database Adapter -- Limited to 1 database target for the database of newScale Request Center for Cloud.

If additional licenses are required beyond these quantities, a separate purchase and installation of CPO is required.

Cisco Service Connector and Adapters restricted to use with Cisco Cloud Portal.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Cisco Cloud Network Automation Provisioner (CNAP)

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

Additional Definitions

“**Authorized Tenant**” means a user (business entity) that has been authorized by Customer to use a particular Network Container.

“**CNAP**” means the Cisco Cloud Network Automation Provisioner software.

“**CNAP Administrator Portal**” means the administrator portal in CNAP utilized by Customer for administrative purposes.

“**CNAP Tenant Portal**” means the tenant portal in CNAP utilized by Authorized Tenants to subscribe to service plans published by Customer, create or decommission their Network Containers and refine policy as permitted by the service plan.

“**Included Programs**” means any separate software programs or components that are distributed by Cisco bundled with CNAP. For example, Cisco may provide a version of Cisco Network Services Orchestrator software (“NSO”) with CNAP. Included Programs are exclusively for use by CNAP.

"**License Term**" means the period of time during which Customer is authorized by Cisco to use the Software. Such period of time will be indicated in the description associated with the Cisco product identification number for the applicable Software license purchased by Customer from an Approved Source.

"Network Container" means a grouping of network services that may be selected from a catalog made available via the CNAP Administrator Portal. The catalog may be updated by Cisco from time to time at its sole discretion. For example, a Network Container may contain the following components: a virtualized network segment connecting to a tier of applications and firewall and security policies. CNAP counts and displays in the CNAP Administrator Portal the number of Network Containers that have been created using CNAP and subscribed to by Authorized Tenants for their use.

"**Software**" means CNAP and any Included Programs.

Additional License Terms and Conditions

1. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco hereby grants to Customer, during the License Term, a nonexclusive and nontransferable right solely to (i) install a single copy of the Software on an active server and up to two additional copies of the Software on standby servers (each owned or leased by Customer) to enable a high availability implementation, (ii) use the Software to create and configure Network Containers, and (iii) permit its Authorized Tenants to subscribe to and use the number of Network Containers for which Customer has paid the required license fees to an Approved Source.
2. Each Network Container must be created and configured using CNAP.
3. Customer may create and configure a Network Container on behalf of an Authorized Tenant or permit an Authorized Tenant to create and configure a Network Container on its own behalf utilizing the CNAP Tenant Portal.
4. Customer is responsible for ensuring that Customer and its Authorized Tenants do not subscribe to or use more than the number of Network Containers for which Customer has paid the required license fees to an Approved Source.
5. Customer may only access or interface with the Software by means of the CNAP Administrator Portal to define and publish service plans and configure and operate the network service functions of network elements registered within CNAP. Only Customer is permitted to use the CNAP Administrator Portal. Authorized Tenants may only access the Software through the CNAP Tenant Portal.
6. CNAP and the Included Programs may not be used independently from one another. The Included Programs may only be used to directly execute the commands initiated through the CNAP Administrator Portal. The Software may not be used to manage, monitor, configure, operate or otherwise interface with any network element, device, function or service other than those directly enabled via CNAP.
7. Network elements and their associated functionality are constantly evolving, and therefore, the Software may not support all devices, capabilities or use cases.
8. Upon termination or expiration of the License Term, Customer shall cease all use of the Software (including the creation or use of any Network Containers).

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Supplemental End User License Agreement for Cisco Collaborative Knowledge

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement (“SEULA”) contains additional terms and conditions for the Software licensed under the End User License Agreement (“EULA”) between you and Cisco. Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA, which you acknowledge and agree that your access and use of Cisco Collaborative Knowledge (the “Software”), is subject to the terms and conditions provided in this SEULA and the **Cisco Universal Cloud Services Agreement** located at http://www.cisco.com/go/legal, which may be updated from time to time by Cisco.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THESE TERMS AND CONDITIONS, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") AS SET FORTH HEREIN.

1. The Software. Cisco Collaborative Knowledge is an enterprise collaboration platform that may provide different functionality, including, but not limited to: content/documents (content development, content management, portals, and Intranets); communication (voice/video, instant messaging, conferencing, and email); business process (business applications, vertical applications, customer care, and workflow); and social networking (profiles, teams, communities, networks).
2. Third Party Offerings. Certain uses of the Software may allow Customer to evaluate and use third party applications, content and/or services made available either within or outside of Cisco Collaborative Knowledge (“Third Party Offerings”). Customer’s use of Third Party Offerings will be governed by terms between the Third Party and Customer, which Customer must accept before the installing, uploading, display or in any way using such Third Party Offerings in connection with Cisco Collaborative Knowledge. Questions about the terms should be addressed directly to the Third Party Offering provider. Third Party Offerings may involve the exchange of data with Cisco Collaborative Knowledge. Cisco is not responsible for Customer’s data exchanged with Third Parties or for modifications or deletions of Customer’s data made by third parties or Third Party Offerings. If Customer has questions or concerns about the processing or handling of Customer’s data by Third Party Offering providers, Customer should contact those providers directly. Customer bears all risks associated with using or relying upon Third Party Offerings. Cisco and the Third Party Offering provider do not warrant the accuracy, reliability, completeness, usefulness, non-infringement, or quality of any Third Party Offerings and hereby disclaim all express and implied warranties, including any implied warranties of merchantability or fitness for a particular purpose, relating to such Third Party Offerings. Cisco and the Third Party Offering provider shall not be liable or responsible in any way for any losses or damage of any kind, including lost profits or other indirect or consequential damages, relating to Customer’s use of or reliance upon any Third Party Offering. Customer acknowledges that all third party licensors and suppliers retain all right, title and interest in third party software and all copies thereof, including all copyright and other intellectual property rights.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

1. ADDITIONAL LICENSE RESTRICTIONS
Software Upgrades, Major and Minor Releases
Cisco may provide Cisco Configuration Engine software updates. The software update and new version releases can be purchased through Cisco or a recognized partner or reseller.

The customer should purchase one software update for each Configuration Engine installation. If the customer is eligible to receive the software update or new version release through a Cisco extended service program, the customer should request to receive only one software update or new version release per valid service contract.

Reproduction and Distribution. Customer may not reproduce nor distribute software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS
Please refer to the Cisco Systems, Inc. End User License Agreement.

SO#: xxxxxx - Line#: xx - Ship Set: xx

♻Printed in the USA.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement (“SEULA”) contains additional terms and conditions for the Software Product licensed under the End User License Agreement (“EULA”) between you and Cisco (collectively, the “Agreement”). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, “CUSTOMER”) TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: Cisco Network Active Abstraction

Additional Licensing Instructions:
Client Licensing: To activate the additional users for the licenses purchased please contact your Cisco Account Manager or Sales Representative or send email to ask-ana-licensing@cisco.com with the requested information below:

1. SO/PO Order
2. Your Contact Information
3. Your Cisco Sales Representative Name

NOTE: This alias is used only for license activation. For any questions or support issues, contact your Cisco Account Manager or representative.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Installation and Use
This license strictly prohibits Customer and any user from utilizing this Software for more than a single Customer network management environment.

Reproduction and Distribution
Customer may not reproduce nor distribute software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS
Please refer to the Cisco Systems, Inc. End User License Agreement.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

(This section shall replace the "License" section in the EULA)
License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for the purpose of delivering Managed Services the Software and the Documentation for which Customer has paid the required license fees. "Managed Services" means the performance by Customer of managed services for third parties (Subscribers) which will require communicating with and managing Cisco equipment not owned or leased by the Customer. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by Cisco with the Software in any manner (including on CD Rom, or on line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer s copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer s license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement, or in the applicable purchase order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee (the "Purchase Order").

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation or the applicable Supplemental License Agreement permits installation on non Cisco equipment) for communication with Cisco equipment not owned or leased by Customer in connection with Customer s provision of Managed Services to Subscriber. No other licenses are granted by implication, estoppel or otherwise. Upon termination of Managed Services to Subscriber, Customer is required to remove all deployed Software deployed by Customer to Subscriber s network and servers.

Customer s license to use the Software is contingent upon Customer deploying or otherwise making available the Software and any Documentation in compliance with and subject to the Software Subscriber License Responsibilities listed below.

Software Subscriber License Responsibilities
The following license terms and responsibilities, substantially as stated here, will be accepted and agreed to, in writing or as otherwise provided in the EULA, by the Subscribers of Managed Services:

Subscriber agrees to be bound by the following terms and conditions. In the absence of a signed agreement, use of the Software by Subscriber or by Customer on Subscriber s behalf, or receipt by Subscriber of any direct or indirect benefit derived there from, shall constitute acceptance by Subscriber of the following terms:

1. Subscriber is granted a limited license from Cisco and its suppliers and licensors to use the Software solely in connection with the Managed Services and to the extent such Software is deployed by Customer on Subscriber s network or servers.
2. Upon termination of services to Subscriber, Customer is required to remove, and cooperate with Customer s efforts to remove, all deployed Software from the Subscriber s network and servers.
3. Subscriber may use the Software only in connection with the receipt of Managed Services from Customer, and for the purposes described in the Software s supporting Documentation if any.
4. Subscribers may only use the Software pursuant to these terms and Customer s license with Cisco and its suppliers and licensors, and Subscriber agrees to be governed by such terms and license including without limitation, the General Terms Applicable to the Limited Warranty Statement and End User License Agreement;.
5. Subscriber may receive, or have deployed on its network or servers, updates, patches, error corrections or new or modified versions of the Software (collectively referred to as "Releases") from time to time. Releases are deemed part of the Software subject to the terms herein and the license with Cisco and its suppliers and licensors.
6. Subscribers acknowledge that all right, title and interest in and to the Software, the ideas and expressions contained therein, all updates and enhancements, all physical forms, regardless of where resident, whether permanent or transient, including authorized and unauthorized copies, any and all modifications made by Cisco, its suppliers and licensors, the software s supporting documentation, and all copyrights, patents, trademarks, service marks or other intellectual property or proprietary rights relating to the above are, and shall remain with Cisco and its suppliers and licensors. Subscriber is granted only a limited right of use as set forth herein;.
7. Subscribers will not distribute, provide or make available, either directly or indirectly, to any person, organization or entity, any part of the Software, including but not limited to the code and the software s supporting documentation in any form except as directed by Customer in support of the delivery of Managed Services:.
8. Subscribers will not place any portion of the Software into the public domain; And,
9. Subscribers will not copy, alter, translate, decompile, disassemble, reverse engineer or create derivative works of the Software, except that the Subscriber may make copies as required for the authorized use of the Software, may make copies of the supporting documentation as needed, and may make one additional copy of the Software for back up or archival purposes.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO SYSTEMS SOFTWARE

IMPORTANT READ CAREFULLY: This Supplemental End User License Agreement (SEULA) contains additional terms and conditions for the Software licensed under the End User License Agreement (EULA) between you and Cisco (collectively, the Agreement). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence. In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

ORIGINAL END USER PURCHASER.

ADDITIONAL LICENSE RESTRICTIONS

Device Restricted Versions: Customer may install and run the Software on a single server to manage up to the cumulative device count specified in the Right To Use statement located on the Claim Certificate received as part of the software package. When used anywhere in this SEULA, a "device" means any device in the Customer's network environment which has its own IP address. Please refer to this guide for further device definition.

Customers whose requirements exceed the license limit of devices must purchase additional incremental licenses. Device restrictions are enforced by license registration and through serial key installation.
Limitations associated with the maximum number of devices that the application can support per server is specified below. The licensed device limit will always override the maximum number of devices supported per server unless the customer has purchased and registered the 5,000 or the 10,000 device license offering.

Installation and Use

The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Some license terms, such as device count and proof of preexisting licenses may be electronically enforced. Customer may install and use the following Software components:

Cisco Prime LAN Management Solution (Cisco Prime LMS): May be installed on one (1) server in Customer's network management environment. Installing the Software and applying a single serial license key to two (2) servers are supported in the 5000 and 10,000 device restricted version, but the cumulative total number of devices supports cannot exceed 5000 and 10,000 respectively per serial license key. When two servers are used to host Cisco Prime LMS, each server should have a copy of the original license key installed on it. Customers should not modify the license file.

Legal restriction concerning the distribution of the Cisco Prime LMS applications is described in the Supplemental License Agreement.

Additional Information for 5,000 Device Restricted Version for LMS 4.2

Users of Cisco Prime LMS 4.2 with 5,000 device restricted licensing may require Cisco Prime LMS to be run on separate servers in order to support a large number of devices or to meet certain performance criteria.

One additional copy of Cisco Prime LMS may be installed on a secondary server provided the customer has purchased and registered the 5,000 device restricted version of the Cisco Prime LMS software. When installed on a secondary server, the cumulative total number of devices supported cannot exceed 5,000 per serial license key. Device support beyond 5,000 unique cumulative devices will require additional licenses and copies of Cisco Prime LMS to be purchased.

Additional Information for 10,000 Device Restricted Version for LMS 4.2

Users of Cisco Prime LMS 4.2 with 10,000 device restricted licensing often require Cisco Prime LMS to be run on separate servers in order to support a large number of devices or to meet certain performance criteria.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

One additional copy of Cisco Prime LMS may be installed on a secondary server provided the customer has purchased and registered the 10,000 device restricted version of the Cisco Prime LMS software. When installed on a secondary server, the cumulative total number of devices supported cannot exceed 10,000 per serial license key. Device support beyond 10,000 unique cumulative devices will require additional licenses and copies of Cisco Prime LMS to be purchased.

Additional Information for RHEL

RHEL distribution that comes along with Cisco Prime LMS 4.2 is solely intended for use by Cisco Prime LMS application alone and customers may not use this for other purposes.

Reproduction and Distribution

Customer may not reproduce nor distribute software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc. Software License Agreement.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

SUPPLEMENTAL LICENSE AGREEMENT

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO PRIME CENTRAL

IMPORTANT-READ CAREFULLY: This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND,

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

ADDITIONAL LICENSE RESTRICTIONS
Cisco Prime Central requires a license to connect to and/or interoperate with other Cisco and third party systems or components, and is further subject to the limitations set forth below. Please see the Additional Information section of this document for any licenses which are included with your specific product purchase. If your requirements exceed the scope of any license expressly included with your product, you must purchase additional licenses from Cisco.

The following restrictions apply:

- Cisco Prime Central Tier 1 and Tier 2 Gateway may not be used to connect Cisco Prime Central to third party systems, such as third party trouble ticketing systems, except as expressly licensed as set forth in the Additional Information section or through a separately purchased license.

- Cisco Prime Central Tier 1 and Tier 3 Data Service Adapter instances may only be used to connect to other Cisco applications or components embedded within Cisco applications, and in addition only if expressly licensed as set forth in the Additional Information section or through a separately purchased license.

- Cisco Prime Central may not be integrated with anOSS system(s) using MTOSI interface except as expressly licensed as set forth in the Additional Information section or through a separately purchased license.

- Cisco Prime Central may not be integrated with Cisco Domain Manager(s) except as expressly licensed as set forth in the Additional Information section or through a separately purchased license.

Rights Included for Cisco Prime Central MTOSI License

Cisco Prime Central MTOSI license includes the right to use one (1) MTOSI instance to integrate Cisco Prime Central to an OSS system using the MTOSI interface.

Reproduction and Distribution
Customer may not reproduce nor distribute software.
DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS
Please refer to the Cisco Systems, Inc. Software License Agreement.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

If you have licensed Cisco Workplace Portal, the following additional terms apply:
Cisco Workplace Portal is licensed for use with end user and workplace-related services including non-server computers, computer accessories, PDAs and handhelds, desktop software, mobility, unified communications, end user applications, email management, access to printing or files, office and wireless phones, voicemail, calling cards, video conferencing facilities and other workplace-related services for the greater employee base.
Cisco Service Connectors and Adapters are not for use with the Cisco Workplace Portal.
If you have licensed Cisco Cloud Portal, the following additional terms apply:
Cisco Cloud Portal is licensed for use with cloud computing and data center-related services including compute, storage, network, IaaS, PaaS, application hosting, database services, application development & maintenance, application installations & upgrades, dedicated application hosting, disaster recovery, network administration, application testing, and systems monitoring.

Cisco Cloud Portal is licensed for use only in the management of service catalogues and provisioning of computing and SW components that relate to a cloud computing and orchestration infrastructure maintained and managed by the licensee.

Cisco Service Connector is licensed for the following functions: Core Functions Adapter, Windows Adapter (a single instance for the Windows server hosting the Cisco Process Orchestrator (CPO) Engine), email adapter, single instance of Active Directory (AD)

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Adapter (a single instance for the domain in which the server is installed), Core Automation Pack, Common Activities Automation Pack, and the Tasks Automation Pack.
CPO elements included in Cisco Service Connector can only be used with licensed components listed below:
Cisco Service Connector Web Service Adapter -- Limited to 5 connections to Web Services for newScale Request Center for Cloud and third-party Orchestrators.
Cisco Service Connector Terminal Adapter -- Limited to 1 terminal or UNIX/Linux target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector VMware Adapter -- Limited to 5 connections to VMware vCenter for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Microsoft Community Adapter -- Limited to 1 Windows target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Database Adapter -- Limited to 1 database target for the database of newScale Request Center for Cloud.

If additional licenses are required beyond these quantities, a separate purchase and installation of CPO is required.

Cisco Service Connector and Adapters restricted to use with Cisco Cloud Portal.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

END USER LICENSE AGREEMENT FOR THE TIDAL SOFTWARE PRODUCTS

Software
For purposes of this Supplement, the Software covered under this SEULA includes the following and each of their respective associated components and modules:

Tidal Enterprise Scheduler
Cisco Process Orchestrator
Tidal Performance Analyzer
Cisco Intelligent Automation for Compute
Cisco Intelligent Automation for Cloud
Cisco Intelligent Automation For Cloud Starter Edition
Cisco Server Provisioner
Cisco Intelligent Automation for SAP

Definitions

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

For purposes of this Supplement, the following defined terms will apply:

Designated System shall mean the designated platform for which Customer originally licenses the Software from Cisco for installation and use. Such designated platform may include for instance, but is not limited to, a designation of the specific number of CPUs or system description or name as approved by Cisco.

Movement and Usage Fees shall mean fees applicable as set solely by Cisco for the transfer and installation of Software on a system that is not a Designated System.

Total Deployment Size shall mean the designated configuration for which the Cisco Intelligent Automation For Cloud Starter Edition Solution cannot exceed 160 blades collectively across a customer s installation.

Other Terms and Conditions

Movement and Usage. With respect to the license granted to Customer in the Agreement, such license is applicable only to the Designated System. Movement of Software to another system requires Customer providing prior written notice to obtain updated keys, and additional fees may apply. A fee schedule is available upon Customer s written request to Cisco.

License. For the avoidance of doubt, the license granted to the Software in the license section shall be perpetual if designated as such by Cisco at time of Customer order for the Designated System, subject to payment of any applicable fees, including, but not limited to, any Movement and Usage fees described above.

Total Deployment Size. For avoidance of doubt, no customer shall deploy the Cisco Intelligent Automation For Cloud Starter Edition Solution in a configuration that exceeds 160 blades in total deployment size across their enterprise.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

If you have licensed Cisco Workplace Portal, the following additional terms apply:
Cisco Workplace Portal is licensed for use with end user and workplace-related services including non-server computers, computer accessories, PDAs and handhelds, desktop software, mobility, unified communications, end user applications, email management, access to printing or files, office and wireless phones, voicemail, calling cards, video conferencing facilities and other workplace-related services for the greater employee base.
Cisco Service Connectors and Adapters are not for use with the Cisco Workplace Portal.
If you have licensed Cisco Cloud Portal, the following additional terms apply:
Cisco Cloud Portal is licensed for use with cloud computing and data center-related services including compute, storage, network, IaaS, PaaS, application hosting, database services, application development & maintenance, application installations & upgrades, dedicated application hosting, disaster recovery, network administration, application testing, and systems monitoring.

Cisco Cloud Portal is licensed for use only in the management of service catalogues and provisioning of computing and SW components that relate to a cloud computing and orchestration infrastructure maintained and managed by the licensee.

Cisco Service Connector is licensed for the following functions: Core Functions Adapter, Windows Adapter (a single instance for the Windows server hosting the Cisco Process Orchestrator (CPO) Engine), email adapter, single instance of Active Directory (AD)

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Adapter (a single instance for the domain in which the server is installed), Core Automation Pack, Common Activities Automation Pack, and the Tasks Automation Pack.
CPO elements included in Cisco Service Connector can only be used with licensed components listed below:
Cisco Service Connector Web Service Adapter -- Limited to 5 connections to Web Services for newScale Request Center for Cloud and third-party Orchestrators.
Cisco Service Connector Terminal Adapter -- Limited to 1 terminal or UNIX/Linux target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector VMware Adapter -- Limited to 5 connections to VMware vCenter for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Microsoft Community Adapter -- Limited to 1 Windows target for inbound synchronization of VMware objects to newScale Request Center for Cloud.
Cisco Service Connector Database Adapter -- Limited to 1 database target for the database of newScale Request Center for Cloud.

If additional licenses are required beyond these quantities, a separate purchase and installation of CPO is required.

Cisco Service Connector and Adapters restricted to use with Cisco Cloud Portal.

SO#: xxxxxx - Line#: xx - Ship Set: xx
♻Printed in the USA.

IMPORTANT: READ CAREFULLY

Dear Customer

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

Product Name

R-IOTFND-K9

R-IOTFND-V-K9

This license entitles the user to specific Cisco Field Network Director product features for specific time duration. The specific Cisco Field Network Director product features and the time duration are detailed in the product SKU description above. The user is entitled to receive updates as made available during the term of the license, provided that the user holds a valid license for the application software and there is a valid Cisco SMARTnet or SASU contract on the supporting Field Network Director products.

Additional information regarding the Cisco Field Network Director can be found at: http://www.cisco.com/go/cgnms.

For more information on support and services visit the Cisco Services website at: http://www.cisco.com/go/supportservices

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO WEBEX MEETINGS SERVER SOFTWARE:

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED USB DRIVE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

1. Cisco WebEx Meetings Server (the "Software") is a software-based enterprise conferencing product that integrates audio, video and web conferencing in a single, on-premises solution.

2. License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive, nontransferable and sublicenseable (to Customer's end users) license to use for Customer's (and/or Customer's end users') internal business purposes the Software and Documentation for which Customer has paid the required license and/or subscription fee. The server component of the Software may be installed only on Cisco hardware that is: (a) operated by Customer, or (b) operated by a third party under Customer's direct control. Customer may copy and distribute the client component of the Software to third parties solely and exclusively in connection with allowing such third parties to attend meetings hosted by Customer using the Software, provided that Customer shall remain responsible for such third parties' compliance with the Agreement. "Documentation" means information (whether contained in user or technical manuals, training materials, specifications, videos or otherwise) pertaining to the Software and made available by Cisco with the Software in any manner (including on USB Drive or online). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

3. User Licenses.

"Employees" are the full and part-time employees or third-party contractors of Customer and its subsidiaries, and affiliates. Employees do not include Customer's parent company, unless Customer intends to assign a User account to an Employee of the parent company, which is an option, but requires that the parent company Employee is a User for purposes of usage calculation.

Employees may include third-party contractors, only if (a) Customer allows the third-party contractor to use the Software only for the benefit of Customer, (b) Customer does not charge the third-party contractor for the use of the Software, and (c) Customer shall take full liability for the actions of a third-party contractor, and/or third-party contractor's misuse of the Software.

A "User" is a Customer Employee assigned an account by Customer to use the Software to host meetings. A User may host an unlimited number of meetings ("Meeting(s)") using the Software; provided that a User may only host one (1) Meeting at a time. Each Meeting must be hosted by a User and is limited to the maximum number or participants as determined by the capacity of the Software licensed by Customer.

4. Limited User Licenses. Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, such limitations as are set forth in the SEULA or in the applicable purchase order which has been accepted by Cisco and for which Customer has paid to Cisco the required fee (the "Purchase Order"). Customer may only have as many Users as allowed under any and all applicable Purchase Orders. Customer understands and agrees that the Software will perform internal checks to compare the number of Users using the Software with the number of Users licensed by Customer, and if it repeatedly finds more Users than authorized, the Software may disable itself until such time as Customer purchases additional User licenses.

5. Content. Customer agrees that it is solely responsible for the content of all visual, written or audible communications, files, documents, videos, recordings and any other material ("Content") used, displayed, uploaded, exchanged or transmitted on or through the Software. Under no circumstances will Cisco be liable to Customer for any loss or damages: (i) arising from any Content, or Content related errors or omissions; or (ii) incurred as a result of the use of, access to, or denial of access to the Content.

6. Privacy. Customer understands and agrees that, as part of Cisco providing support to Customer, Cisco may request access to and use of technical or diagnostic information (*e.g.*, server logs) that may contain Personal Information and Non-personal Information of Customer and/or Customer's meeting invitees ("Server Data"). If you provide such Server Data to Cisco, you consent to Cisco's collection, use, processing and storage of Personal Information and Non-personal Information as described below. This Personal Information and Non-personal Information is transferred to Cisco, including the transfer of such information to the United States and/or another country outside the European Economic Area, so Cisco can determine how users are interacting with our products and for the purposes of providing Customer support and

improving our products and services. Cisco may share this information with select third parties in an anonymous aggregated form. None of this Personal Information and Non-personal Information will be used to identify or contact individual users, and use of the Personal Information and Non-personal Information shall be subject to Cisco's Privacy Statement, available at http://www.cisco.com/web/siteassets/legal/privacy.html. Customer may withdraw this consent to collection, use, processing and storage of Personal Information and Non-personal Information at any time by not providing Cisco access to the Server Data. Active steps are required each time by the System Administrator to provide Cisco access to the Server Data.

7. Customer agrees that it will not use the Software to send unsolicited email outside Customer's company or organization (*e.g.*, "spam") in violation of applicable law, falsify any email header information when sending emails (*e.g.*, "spoofing"), or attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity (*e.g.*, "phishing"). Customer further agrees not to use the Software to communicate any message or material that is harassing, libelous, threatening, obscene, or that would violate the intellectual property rights of any party, give rise to civil liability, constitute a criminal offense, or is otherwise unlawful under any applicable law or regulation. Customer agrees to indemnify, defend and hold harmless Cisco from any and all third party claims, liability, damages and/or costs (including, but not limited to, attorneys' fees) arising from Customer's violation of this Section 7.

8. The Software may not be appropriate for use in all countries. Customer agrees that Customer will comply with all applicable laws and regulations in connection with Customer's use of the Software, including, but not limited to: (a) with respect to personally identifiable information sent or received by Customer, all applicable privacy laws and regulations, (b) laws relating to the recording of communications, including, when required, advising all participants in a recorded WebEx Meetings Server meeting or event that the meeting or event is being recorded, and (c) laws relating to the use of VoIP-based services, if applicable. It is the sole responsibility of Customer to ensure it has the right to use all features of the Software in Customer's jurisdiction. Cisco may modify or not make available the Software and/or certain Software features to comply with applicable laws and regulations. The Software is subject to U.S. and local export control laws and regulations. Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of the Software and will obtain all required U.S. and local authorizations, permits, or licenses. Customer certifies that Customer and any third parties Customer invites will not use the Software from within an embargoed country. Customer certifies that they are not on the U.S. Department of Commerce's Denied Persons List or affiliated lists, on the U.S. Department of Treasury's Specially Designated Nationals List or on any U.S. Government export exclusion lists. The export obligations under this clause shall survive the expiration or termination of the Agreement.

9. The Software contains certain third party database products ("Third Party Database Products") that impose additional restrictions on Customer's use. Customer shall not install or configure the Third Party Database Products separately and independently from the Software. Customer shall not access the Third Party Database Products directly or through other database tools, but rather only through the Software. Customer shall not navigate the underlying data schema of the Third Party Database Products. Customer shall not access the Third Party Database Products or

establish the transfer of data without Cisco APIs. Customer shall not upgrade the Third Party Database Products separately, but only as a component of Third Party Database Products.

10. Oracle Java SE Terms and conditions. (i) Trademarks and Logos. This SEULA does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icons including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at http://www.oracle.com/us/legal/third-party-trademarks/index.html; (b) not do anything harmful to or inconsistent with Oracle's rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Customer in any Java Mark. (ii) Third Party Code. Additional copyright notices and license terms applicable to portions of the Oracle Java SE software are set forth in the THIRDPARTYLICENSEREADME.txt file. (iii) Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table 1-1 (Commercial Features in Java SE Production Editions) of the Oracle Java SE software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. (iv) Limited Use. This SEULA does not authorize use of the Oracle Java SE software except with the Software. In addition, this SEULA does not authorize any reconfiguration of the Oracle Java SE software.

11. Portions of the Software utilize Microsoft Windows Media Technologies. Copyright (c) 1999-2006 Microsoft Corporation.

Meraki LLC
500 Terry Francois Blvd.
San Francisco, CA 94158
T 415.432.1000

Last Updated October 13, 2015

Supplemental End User License Agreement

We're excited that you are considering jumping on the Meraki train or have already done so. Meraki's goal, in a word, is to make everything about your experience GREAT. And that means the legal stuff, too. We aim to keep our legal terms simple, transparent, and to the point. This Supplemental End User License Agreement (this "**Agreement**") supplements and amends the terms of the Cisco Systems, Inc. ("**Cisco Systems**") End User License Agreement available at the following web address: http://www.cisco.com/go/eula (the "**EULA**"). This Agreement forms a binding agreement between you, the end user ("**Customer**"), Cisco Systems, and its affiliates, including Meraki LLC, Cisco System's wholly-owned subsidiary ("**Meraki**" together with Cisco Systems and its affiliates, "**Cisco**"), , and it governs your purchase and use of the Cisco Meraki products. Please read this Agreement carefully. By using our products, you acknowledge that you have read, understood, and agree to be bound by this Agreement and to use our products in compliance with this Agreement. Please keep in mind that your use of the Products after changes to this Agreement are published at http://www.cisco.com/web/products/seula/meraki-seula.pdf will constitute your acceptance of the changes. Any material changes are considered effective upon the earlier of (i) your continued use of the Products once you know about the changes, and (ii) 30 days after they are published. If you do not agree to the terms of this Agreement, please do not use our products.

The terms "Customer," "you," "your," and "yours" refer to you, the end customer and user of the Products, whether obtained directly from Cisco or through one of our authorized resellers. The terms "Cisco," "Meraki" "we," "us," and "our" refer to Cisco.

Okay, with all that in mind, let's dive in. Heads-up: there's a glossary of defined terms at the end.

Article 1 Licenses and Restrictions.

1.1. Paid Licenses. Subject to the terms and conditions of this Agreement, all the paperwork related to your purchasing being in order, and you actually paying for the Products, Meraki grants you non-sublicensable, non-exclusive, non-transferable licenses (i) to use the Firmware on the Hardware (the "**Firmware Licenses**"), and (ii) to use the Hosted Software via the Internet (the "**Hosted Software Licenses**"), in each case until the Co-Termination Date or the earlier termination of this Agreement. The Support Services we provide to you are included in the cost of the Hosted Software Licenses. The Firmware License for each item of Hardware you purchase is contingent upon you purchasing and maintaining a valid Hosted Software License, without which the Hardware will not function.

1.2. Third-Party Licenses. If any of the Products include software provided by a third party, the terms under which that software is provided to you may be found at https://meraki.cisco.com/support/#policies:thirdparty. Don't worry, we've made sure you have the right to use any such software as part of the Products at no additional cost to you.

1.3. Restrictions. Let's play nice together. Don't (and don't permit anyone who obtains access to your Network (a "**Network User**") to) directly or indirectly, reverse engineer the Products or otherwise attempt to discover the source code or algorithms of Meraki software or hardware.

1.4. Customer Responsibilities. Similarly, please use the Hardware only in accordance with the specifications (the "**Specifications**") available on our website, and keep in mind that you (not Meraki) are solely responsible for maintaining administrative control over your Hosted Software account. And, of course, it is your responsibility to comply with all applicable laws in your use of the Products.

Article 2 Ownership; Customer Data.

2.1. Meraki Rights. As between you and Meraki, Meraki owns and reserves all rights with respect to the Software and all intellectual property rights with respect to the Hardware. In addition, you hereby assign to Meraki all of your interest in any feedback you convey to us related to the Products. Meraki may incorporate modifications into the Hosted Software, the Firmware and the Documentation at any time.

2.2. Customer Data. By using the Hardware, you understand and agree that you are collecting data regarding the devices that connect to your Network and how your network is being used, including the types of data described below. By means of the Hardware, you are then transferring that data to Meraki for processing and storage, including data that may contain personally identifiable information of your Network Users (collectively, "**Customer Data**"). That said, the Products include functionality that limits or restricts the types of information collected, and you may certainly make use of that functionality. We process and store Customer Data exclusively for the purpose of providing the Products to you, except to the extent necessary to protect our rights in any dispute with you or as required by law. It is your responsibility to provide notice to, and obtain any necessary consents from, your Network Users regarding collection, processing, and storage of Customer Data.

2.2.1. **Traffic Information.** "**Traffic Information**" means information about devices that connect to your Network, such as MAC address, device name, device type, operating system, geolocation information, and information transmitted by devices when attempting to access or download data or content (e.g., hostnames, protocols, port numbers, and IP addresses) via the Network. We process and store Traffic Information on your behalf so you can monitor the use and performance of your Network and exercise control (such as network traffic shaping) over the traffic on your Network.

2.2.2. **CMX.** By enabling and using CMX, you collect the MAC address and relative signal strength of WiFi-enabled devices that are within range of your wireless Network. Meraki does not store these MAC addresses on its servers, except in a de-identified form, and they are not stored on your Hardware. Meraki has no responsibility for whether and how you configure the API to transfer this data to non-Meraki servers or what happens to this data following such a transfer.

2.2.3. **Systems Manager.** If you choose to use Systems Manager, certain agent software must be installed on the mobile devices, laptops or other devices you choose to enroll. You will then, depending on the type of device, be able to perform remotely actions such as accessing and deleting files, tracking location, enforcing policies, and installing and removing apps.

2.3. Publicity. We won't use each other's name or trademarks without written consent, but we may use your company name and logo in customer lists on our website and collateral.

Article 3 Term and Termination.

3.1. Term. This Agreement will be effective until the expiration of the Term (the "**Co-Termination Date**"), unless earlier terminated per Section 3.2, below. If you subsequently purchase additional Hosted Software Licenses, the Co-Termination Date will be adjusted so that all of your Hosted Software Licenses (including the new ones) terminate on the same date. This adjusted Co-Termination Date is calculated by (i) determining the aggregate amount of time that your new Hosted Software Licenses extend past your existing Co-Termination Date, and (ii) distributing that amount of time among all your Hosted Software Licenses (including both new and existing ones) pro rata based on the one-year list price for each type of Hosted Software License. Further information is at http://meraki.cisco.com/support#policies:licensing.

3.2. Termination. You may terminate this Agreement for any reason effective upon 30 days prior written notice to Meraki. Meraki may suspend your use of the Products at any time if Meraki reasonably believes that you have breached the terms of Sections 1.3 and 2.2; if such breach remains uncured for 10 days following receipt of notice from Meraki, then Meraki may terminate this Agreement immediately. You may terminate this Agreement for cause if we breach any material obligation of ours under this Agreement and fail to cure such breach within 10 days following receipt of written notice from you. If you terminate this Agreement for cause, you will receive a refund equal to the value of the remaining time on your Hosted Software Licenses.

3.3. Effect of Termination. Upon any termination of this Agreement, the Hosted Software Licenses and Firmware Licenses will automatically terminate. Sections 2.1 and 4.3, and Article 5 will survive any termination of this Agreement.

Article 4 Warranties; Limitation of Liability.

4.1. Service Level Agreement. Meraki uses its best efforts to keep the Hosted Software up and running 24/7, but no one is perfect. The Service Level Agreement available at https://meraki.cisco.com/trust#sla is your exclusive remedy with respect to any interruptions in the availability of the Hosted Software.

4.2. Hardware Warranties. We represent to you that, during the Warranty Period, the Hardware will be free from material defects in materials and workmanship. Hardware not meeting the warranty above will be, at our option, (a) repaired, (b) replaced, or (c) if you are the original purchaser, we will refund the depreciated amount of the price you paid for such Hardware, calculated on a straight-line, five-year basis. All Hardware repaired or replaced under warranty will be warranted for the remainder of the Warranty Period. For any return permitted under Meraki's then-current return policy (available at http://meraki.cisco.com/support/#policies:return), you will request a Return Materials Authorization ("**RMA**") number in writing with the reasons for the return request. The warranties in this

Section are subject to our Product End of Life Policy, available at https://meraki.cisco.com/support/#policies:eol. "**Warranty Period**" means the greater of one year or the warranty period set forth in the applicable Specification, commencing, in either case, on the date Hardware is shipped to the original customer. This Section 4.2 is our sole liability and your sole remedy for any breach of warranty by Meraki.

4.3. Disclaimer of Warranties. Except as set forth in Sections 4.1 and 4.2, Meraki disclaims all warranties, express, implied, statutory, or otherwise, including any implied warranty of merchantability, fitness for a particular purpose, non-infringement, or title. Meraki assumes no responsibility for any damages to Customer's hardware, software, or other materials.

Article 5 Indemnity. Customer will indemnify Meraki, its affiliates, and their employees, officers, directors, successors, assigns, agents for all losses (including reasonable attorneys' fees) relating to any claims brought by a third party to the extent based upon: (i) grossly negligent or intentionally wrongful acts of Customer or Customer's assistants, employees, agents, or Network Users; (ii) Customer's unauthorized modification of the Products; (iii) Customer's combination of the Products with other products, software, or services not supplied or specified by Meraki; or (iv) Customer's failure to implement software modifications or patches provided by Meraki within a reasonable timeframe.

Article 6 Miscellaneous. This Agreement and the EULA constitute the entire agreement between you and us and supersede all prior agreements and understandings about all this stuff. Failure to exercise any right under this Agreement will not constitute a waiver. There are no third-party beneficiaries to this Agreement. This Agreement is governed by the laws of California without reference to conflicts of law rules. For any dispute relating to this Agreement, the Parties consent to personal jurisdiction and the exclusive venue of the courts in Santa Clara County, California. Communications we send to you electronically will be deemed to be in writing. Any notice you provide to us under this Agreement will be in writing and sent by overnight courier or certified mail (receipt requested) to the address above. If any provision of this Agreement is found unenforceable, this Agreement will be construed as if it had not been included. Meraki may assign this Agreement without the consent of Customer to Cisco Systems, Inc. or its affiliates. If there is a conflict between the terms of this Agreement and the EULA, the terms of this Agreement will apply.

Article 7 Certain Definitions. The following terms not defined elsewhere in this Agreement have the respective meanings set forth below.

"**CMX**" means the Connected Mobile Experience (CMX) features of the Hosted Software.

"**Documentation**" means any user instructions, manuals, Specifications, or other documentation provided by Meraki at https://meraki.cisco.com/support/#documentation that relate to the Products, including any Modifications.

"**Firmware**" means software embedded in or otherwise running on the Hardware.

"**Hardware**" means Meraki hardware products you have purchased, received in a free trial, promotion, or beta test, or otherwise running on your Network.

“**Hosted Software**” means our proprietary, web-based software platform, including the interface known as the ”Dashboard,” Systems Manager and any API provided by Meraki.

“**Network**” means your local area network, created in whole or in part by use of the Products.

“**Products**” means the Hardware, the Hosted Software, the Firmware, the Documentation, and the Support Services.

“**Support Services**” means the customer support services described at http://meraki.cisco.com/support

“**Systems Manager**” means Meraki’s web-based mobile device management software.

“**Term**” means the term of the Hosted Software Licenses you have purchased or received in a free trial, as modified each time you purchase additional Hosted Software Licenses so that all your Hosted Software Licenses expires at the same time in accordance with the provisions of Section 3.1.

Cisco Network Services Orchestrator (NSO)
Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("**SEULA**") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("**EULA**") between Customer and Cisco (collectively, the "**Agreement**"). Capitalized terms used in this SEULA but not defined herein will have the meanings ascribed to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA regarding Customer's rights to access and use the Software, Customer agrees to comply at all times with the terms and conditions of this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND CUSTOMER IS BINDING ITSELF TO THE TERMS AND CONDITIONS OF THE AGREEMENT. IF CUSTOMER DOES NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO CUSTOMER, AND (I) CUSTOMER MAY NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE; (II) CUSTOMER MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGING AND ANY WRITTEN MATERIALS FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, CUSTOMER MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. CUSTOMER'S RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF CUSTOMER IS THE ORIGINAL END USER PURCHASER.

Product Name: Cisco Network Services Orchestrator (NSO)

NSO Non-Production Network License

If the Cisco Network Services Orchestrator ("**NSO**") software (the "**Software**") is used solely to configure, manage, or interface with ("**Manage**") network devices or other systems (physical or virtual) (together, "**Network Elements**") in a testing, validation, or laboratory environment (a "**Lab**" or "**Non-Production Network**"), the Customer requires at least one (1) of each of the following to obtain a valid license to use the Software:

- A Cisco NSO server Lab license for each copy of the Cisco NSO server software loaded into memory (an "**Active NSO Lab Server**").
- A network element driver ("**NED**") license per NED type for each Active NSO Lab Server.
  - For clarity, NEDs enable the management of Network Elements running the same embedded software type; e.g., there is a NED for Cisco IOS devices, another NED for IOS XR devices, and a NED for JunOS devices.

NSO Production Network License

If the Software is used to Manage Network Elements that are **not solely for Lab use**, the Customer requires at least one (1) of each of the following to obtain a valid license to use the Software:

- A Cisco NSO server license for each copy of the Cisco NSO server software loaded into memory (an "**Active NSO Server**");
- A right to use ("**RTU**") license for each managed physical device;

- A RTU license for each CPU core (physical or virtual) used by a managed virtual network function (“**VNF**”) or software application;
- A NED license per NED type for each Active NSO Server.
    - Additional NED licenses are not required for high availability standby servers

- If a high availability implementation of Cisco NSO is desired, at least one (1) high availability license for each standby server is also required.

Independent Development

Any products, software or technologies that either party may design or develop that rely on the Software, and any intellectual property rights arising therefrom, will not impair the other party’s right to independently design, develop, license or use commercial products and offerings that rely on the Software.

NSO Pricing

Any contractual Cisco price list discounts to which Customer may otherwise be entitled do not apply to the purchase of licenses for the Software or its associated support.

Disclaimer Regarding NEDs

NEDs provide the connectivity between Cisco NSO and Network Elements. Network Elements and their associated functionality are constantly evolving and, therefore, it is not guaranteed that NEDs will support all possible devices, capabilities, or use cases. Customers may request additional NED functionality from Cisco by discussing with their Cisco Sales representative, or may choose to develop their own NEDs using documented Cisco NSO APIs.

Meraki LLC
500 Terry Francois Blvd.
San Francisco, CA 94158
T 415.432.1000

Last Updated October 13, 2015

Supplemental End User License Agreement

We're excited that you are considering jumping on the Meraki train or have already done so. Meraki's goal, in a word, is to make everything about your experience GREAT. And that means the legal stuff, too. We aim to keep our legal terms simple, transparent, and to the point. This Supplemental End User License Agreement (this "**Agreement**") supplements and amends the terms of the Cisco Systems, Inc. ("**Cisco Systems**") End User License Agreement available at the following web address: http://www.cisco.com/go/eula (the "**EULA**"). This Agreement forms a binding agreement between you, the end user ("**Customer**"), Cisco Systems, and its affiliates, including Meraki LLC, Cisco System's wholly-owned subsidiary ("**Meraki**" together with Cisco Systems and its affiliates, "**Cisco**"), , and it governs your purchase and use of the Cisco Meraki products. Please read this Agreement carefully. By using our products, you acknowledge that you have read, understood, and agree to be bound by this Agreement and to use our products in compliance with this Agreement. Please keep in mind that your use of the Products after changes to this Agreement are published at http://www.cisco.com/web/products/seula/meraki-seula.pdf will constitute your acceptance of the changes. Any material changes are considered effective upon the earlier of (i) your continued use of the Products once you know about the changes, and (ii) 30 days after they are published. If you do not agree to the terms of this Agreement, please do not use our products.

The terms "Customer," "you," "your," and "yours" refer to you, the end customer and user of the Products, whether obtained directly from Cisco or through one of our authorized resellers. The terms "Cisco," "Meraki" "we," "us," and "our" refer to Cisco.

Okay, with all that in mind, let's dive in. Heads-up: there's a glossary of defined terms at the end.

Article 1 Licenses and Restrictions.

1.1. **Paid Licenses**. Subject to the terms and conditions of this Agreement, all the paperwork related to your purchasing being in order, and you actually paying for the Products, Meraki grants you non-sublicensable, non-exclusive, non-transferable licenses (i) to use the Firmware on the Hardware (the "**Firmware Licenses**"), and (ii) to use the Hosted Software via the Internet (the "**Hosted Software Licenses**"), in each case until the Co-Termination Date or the earlier termination of this Agreement. The Support Services we provide to you are included in the cost of the Hosted Software Licenses. The Firmware License for each item of Hardware you purchase is contingent upon you purchasing and maintaining a valid Hosted Software License, without which the Hardware will not function.

1.2. Third-Party Licenses. If any of the Products include software provided by a third party, the terms under which that software is provided to you may be found at https://meraki.cisco.com/support/#policies:thirdparty. Don't worry, we've made sure you have the right to use any such software as part of the Products at no additional cost to you.

1.3. Restrictions. Let's play nice together. Don't (and don't permit anyone who obtains access to your Network (a "**Network User**") to) directly or indirectly, reverse engineer the Products or otherwise attempt to discover the source code or algorithms of Meraki software or hardware.

1.4. Customer Responsibilities. Similarly, please use the Hardware only in accordance with the specifications (the "**Specifications**") available on our website, and keep in mind that you (not Meraki) are solely responsible for maintaining administrative control over your Hosted Software account. And, of course, it is your responsibility to comply with all applicable laws in your use of the Products.

Article 2 Ownership; Customer Data.

2.1. Meraki Rights. As between you and Meraki, Meraki owns and reserves all rights with respect to the Software and all intellectual property rights with respect to the Hardware. In addition, you hereby assign to Meraki all of your interest in any feedback you convey to us related to the Products. Meraki may incorporate modifications into the Hosted Software, the Firmware and the Documentation at any time.

2.2. Customer Data. By using the Hardware, you understand and agree that you are collecting data regarding the devices that connect to your Network and how your network is being used, including the types of data described below. By means of the Hardware, you are then transferring that data to Meraki for processing and storage, including data that may contain personally identifiable information of your Network Users (collectively, "**Customer Data**"). That said, the Products include functionality that limits or restricts the types of information collected, and you may certainly make use of that functionality. We process and store Customer Data exclusively for the purpose of providing the Products to you, except to the extent necessary to protect our rights in any dispute with you or as required by law. It is your responsibility to provide notice to, and obtain any necessary consents from, your Network Users regarding collection, processing, and storage of Customer Data.

2.2.1. **Traffic Information.** "**Traffic Information**" means information about devices that connect to your Network, such as MAC address, device name, device type, operating system, geolocation information, and information transmitted by devices when attempting to access or download data or content (e.g., hostnames, protocols, port numbers, and IP addresses) via the Network. We process and store Traffic Information on your behalf so you can monitor the use and performance of your Network and exercise control (such as network traffic shaping) over the traffic on your Network.

2.2.2. **CMX.** By enabling and using CMX, you collect the MAC address and relative signal strength of WiFi-enabled devices that are within range of your wireless Network. Meraki does not store these MAC addresses on its servers, except in a de-identified form, and they are not stored on your Hardware. Meraki has no responsibility for whether and how you configure the API to transfer this data to non-Meraki servers or what happens to this data following such a transfer.

2.2.3. **Systems Manager.** If you choose to use Systems Manager, certain agent software must be installed on the mobile devices, laptops or other devices you choose to enroll. You will then, depending on the type of device, be able to perform remotely actions such as accessing and deleting files, tracking location, enforcing policies, and installing and removing apps.

2.3. Publicity. We won't use each other's name or trademarks without written consent, but we may use your company name and logo in customer lists on our website and collateral.

Article 3 Term and Termination.

3.1. Term. This Agreement will be effective until the expiration of the Term (the "**Co-Termination Date**"), unless earlier terminated per Section 3.2, below. If you subsequently purchase additional Hosted Software Licenses, the Co-Termination Date will be adjusted so that all of your Hosted Software Licenses (including the new ones) terminate on the same date. This adjusted Co-Termination Date is calculated by (i) determining the aggregate amount of time that your new Hosted Software Licenses extend past your existing Co-Termination Date, and (ii) distributing that amount of time among all your Hosted Software Licenses (including both new and existing ones) pro rata based on the one-year list price for each type of Hosted Software License. Further information is at http://meraki.cisco.com/support#policies:licensing.

3.2. Termination. You may terminate this Agreement for any reason effective upon 30 days prior written notice to Meraki. Meraki may suspend your use of the Products at any time if Meraki reasonably believes that you have breached the terms of Sections 1.3 and 2.2; if such breach remains uncured for 10 days following receipt of notice from Meraki, then Meraki may terminate this Agreement immediately. You may terminate this Agreement for cause if we breach any material obligation of ours under this Agreement and fail to cure such breach within 10 days following receipt of written notice from you. If you terminate this Agreement for cause, you will receive a refund equal to the value of the remaining time on your Hosted Software Licenses.

3.3. Effect of Termination. Upon any termination of this Agreement, the Hosted Software Licenses and Firmware Licenses will automatically terminate. Sections 2.1 and 4.3, and Article 5 will survive any termination of this Agreement.

Article 4 Warranties; Limitation of Liability.

4.1. Service Level Agreement. Meraki uses its best efforts to keep the Hosted Software up and running 24/7, but no one is perfect. The Service Level Agreement available at https://meraki.cisco.com/trust#sla is your exclusive remedy with respect to any interruptions in the availability of the Hosted Software.

4.2. Hardware Warranties. We represent to you that, during the Warranty Period, the Hardware will be free from material defects in materials and workmanship. Hardware not meeting the warranty above will be, at our option, (a) repaired, (b) replaced, or (c) if you are the original purchaser, we will refund the depreciated amount of the price you paid for such Hardware, calculated on a straight-line, five-year basis. All Hardware repaired or replaced under warranty will be warranted for the remainder of the Warranty Period. For any return permitted under Meraki's then-current return policy (available at http://meraki.cisco.com/support/#policies:return), you will request a Return Materials Authorization ("**RMA**") number in writing with the reasons for the return request. The warranties in this

2.2.3. **Systems Manager.** If you choose to use Systems Manager, certain agent software must be installed on the mobile devices, laptops or other devices you choose to enroll. You will then, depending on the type of device, be able to perform remotely actions such as accessing and deleting files, tracking location, enforcing policies, and installing and removing apps.

2.3. Publicity. We won't use each other's name or trademarks without written consent, but we may use your company name and logo in customer lists on our website and collateral.

Article 3 Term and Termination.

3.1. Term. This Agreement will be effective until the expiration of the Term (the "**Co-Termination Date**"), unless earlier terminated per Section 3.2, below. If you subsequently purchase additional Hosted Software Licenses, the Co-Termination Date will be adjusted so that all of your Hosted Software Licenses (including the new ones) terminate on the same date. This adjusted Co-Termination Date is calculated by (i) determining the aggregate amount of time that your new Hosted Software Licenses extend past your existing Co-Termination Date, and (ii) distributing that amount of time among all your Hosted Software Licenses (including both new and existing ones) pro rata based on the one-year list price for each type of Hosted Software License. Further information is at http://meraki.cisco.com/support#policies:licensing.

3.2. Termination. You may terminate this Agreement for any reason effective upon 30 days prior written notice to Meraki. Meraki may suspend your use of the Products at any time if Meraki reasonably believes that you have breached the terms of Sections 1.3 and 2.2; if such breach remains uncured for 10 days following receipt of notice from Meraki, then Meraki may terminate this Agreement immediately. You may terminate this Agreement for cause if we breach any material obligation of ours under this Agreement and fail to cure such breach within 10 days following receipt of written notice from you. If you terminate this Agreement for cause, you will receive a refund equal to the value of the remaining time on your Hosted Software Licenses.

3.3. Effect of Termination. Upon any termination of this Agreement, the Hosted Software Licenses and Firmware Licenses will automatically terminate. Sections 2.1 and 4.3, and Article 5 will survive any termination of this Agreement.

Article 4 Warranties; Limitation of Liability.

4.1. Service Level Agreement. Meraki uses its best efforts to keep the Hosted Software up and running 24/7, but no one is perfect. The Service Level Agreement available at https://meraki.cisco.com/trust#sla is your exclusive remedy with respect to any interruptions in the availability of the Hosted Software.

4.2. Hardware Warranties. We represent to you that, during the Warranty Period, the Hardware will be free from material defects in materials and workmanship. Hardware not meeting the warranty above will be, at our option, (a) repaired, (b) replaced, or (c) if you are the original purchaser, we will refund the depreciated amount of the price you paid for such Hardware, calculated on a straight-line, five-year basis. All Hardware repaired or replaced under warranty will be warranted for the remainder of the Warranty Period. For any return permitted under Meraki's then-current return policy (available at http://meraki.cisco.com/support/#policies:return), you will request a Return Materials Authorization ("**RMA**") number in writing with the reasons for the return request. The warranties in this

Section are subject to our Product End of Life Policy, available at https://meraki.cisco.com/support/#policies:eol. "**Warranty Period**" means the greater of one year or the warranty period set forth in the applicable Specification, commencing, in either case, on the date Hardware is shipped to the original customer. This Section 4.2 is our sole liability and your sole remedy for any breach of warranty by Meraki.

4.3. Disclaimer of Warranties. Except as set forth in Sections 4.1 and 4.2, Meraki disclaims all warranties, express, implied, statutory, or otherwise, including any implied warranty of merchantability, fitness for a particular purpose, non-infringement, or title. Meraki assumes no responsibility for any damages to Customer's hardware, software, or other materials.

Article 5 Indemnity. Customer will indemnify Meraki, its affiliates, and their employees, officers, directors, successors, assigns, agents for all losses (including reasonable attorneys' fees) relating to any claims brought by a third party to the extent based upon: (i) grossly negligent or intentionally wrongful acts of Customer or Customer's assistants, employees, agents, or Network Users; (ii) Customer's unauthorized modification of the Products; (iii) Customer's combination of the Products with other products, software, or services not supplied or specified by Meraki; or (iv) Customer's failure to implement software modifications or patches provided by Meraki within a reasonable timeframe.

Article 6 Miscellaneous. This Agreement and the EULA constitute the entire agreement between you and us and supersede all prior agreements and understandings about all this stuff. Failure to exercise any right under this Agreement will not constitute a waiver. There are no third-party beneficiaries to this Agreement. This Agreement is governed by the laws of California without reference to conflicts of law rules. For any dispute relating to this Agreement, the Parties consent to personal jurisdiction and the exclusive venue of the courts in Santa Clara County, California. Communications we send to you electronically will be deemed to be in writing. Any notice you provide to us under this Agreement will be in writing and sent by overnight courier or certified mail (receipt requested) to the address above. If any provision of this Agreement is found unenforceable, this Agreement will be construed as if it had not been included. Meraki may assign this Agreement without the consent of Customer to Cisco Systems, Inc. or its affiliates. If there is a conflict between the terms of this Agreement and the EULA, the terms of this Agreement will apply.

Article 7 Certain Definitions. The following terms not defined elsewhere in this Agreement have the respective meanings set forth below.

"**CMX**" means the Connected Mobile Experience (CMX) features of the Hosted Software.

"**Documentation**" means any user instructions, manuals, Specifications, or other documentation provided by Meraki at https://meraki.cisco.com/support/#documentation that relate to the Products, including any Modifications.

"**Firmware**" means software embedded in or otherwise running on the Hardware.

"**Hardware**" means Meraki hardware products you have purchased, received in a free trial, promotion, or beta test, or otherwise running on your Network.

"**Hosted Software**" means our proprietary, web-based software platform, including the interface known as the "Dashboard," Systems Manager and any API provided by Meraki.

"**Network**" means your local area network, created in whole or in part by use of the Products.

"**Products**" means the Hardware, the Hosted Software, the Firmware, the Documentation, and the Support Services.

"**Support Services**" means the customer support services described at http://meraki.cisco.com/support

"**Systems Manager**" means Meraki's web-based mobile device management software.

"**Term**" means the term of the Hosted Software Licenses you have purchased or received in a free trial, as modified each time you purchase additional Hosted Software Licenses so that all your Hosted Software Licenses expires at the same time in accordance with the provisions of Section 3.1.