Contract # AR2470

STATE OF UTAH COOPERATIVE CONTRACT

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

AT&T Corp.		
Name		
One AT&T Way		
Address		
Bedminster	NJ	07921-0752
City	State	Zip

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

Contact Person Donnie Powell Phone # 214-208-2353 Email dp1416@att.com
Vendor # vc0000146443 Commodity Code #920-05

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

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

4. CONTRACT PERIOD: Effective Date: 9/15/2017 Termination Date: 9/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Pursuant to Solicitation #CH16012, Contractor must re-certify its qualifications each year.

5. Administrative Fee, as described Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, an administrative fee of one-quarter of one percent (0.25% or 0.0025) of the total billed charges (after the application of all discounts and credits) which are invoiced to Purchasing Entities (exclusive of taxes, surcharges, and fees) for the Services provided under the Master Agreement (the "NASPO ValuePoint Administrative Fee"). The NASPO ValuePoint Administrative Fee shall be submitted quarterly, no later than sixty (60) days following the end of each calendar quarter.

6. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions, including three (3) attached Exhibits
ATTACHMENT B: Data Security Addendum
ATTACHMENT C: Scope of Services Awarded to Contractor
ATTACHMENT D: Pricing Discounts Attachment
ATTACHMENT E: Contractor's Response to the Solicitation

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, Procurement Rules, and Contractor's response to Bid #CH16012.

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

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

CONTRACTOR

Contractor's signature — Date: 09/13/17

Matt Hickey, VP Public Sector Channel Marketing
Type or Print Name and Title

STATE

for Director, Division of Purchasing — Date: 9.15.2017

Solomon Kingston	801-538-3228	801-538-3882	skingston@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. MASTER AGREEMENT; ORDER OF PRECEDENCE

(A) The Master Agreement consists of the documents set forth in §1(A)(2) through §1(A)(8) below (the "Master Agreement"). A valid Participating Addendum combined with the Master Agreement constitutes the full agreement between Contractor and the corresponding Participating Entity and it's Purchasing Entities (the "Agreement"). In the event of any conflict between the documents comprising the Agreement the following constitutes the order of precedence:

(1) The Purchasing Entity's applicable Participating Addendum;
(2) The Master Agreement (i.e., the Cover Page);
(3) Attachment A to the Master Agreement, including Exhibits 1-3 (the "Terms and Conditions");
(4) Attachment B to the Master Agreement (the "Data Security Addendum");
(5) Attachment C to the Master Agreement (the "Scope of Services Awarded to Contractor");
(6) Attachment D to the Master Agreement (the "Pricing Discounts Attachment");
(7) Attachment E to the Master Agreement ("Contractor's Response to the Solicitation"); and
(8) The Solicitation

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

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

- **Acceptable Use Policy and AUP** mean Contractor's Acceptable Use Policy which applies to (A) Services provided over or accessing the Internet and (B) wireless (i.e., cellular) data and messaging Services. The AUP can be found at www.att.com/aup or other locations Contractor may designate.

- **Administrative Fee** means the NASPO ValuePoint administrative fee as more fully described in §27.

- **Affiliate** of a party means any entity that controls, is controlled by or is under common control with such party.

- **Agreement** has the definition set forth in §1(A) above.

- **API** means an application program interface used to make a resources request from a remote implementer program. An API may include coding, specifications for routines, data structures, object classes, and protocols used to communicate between programs.

- **Confidential Information** means: (A) information the parties or their Affiliates share with each other in connection with this Agreement or in anticipation of providing Services under this Agreement (including pricing or other proposals), but only to the extent identified as Confidential Information in writing; and (B) except as may be required by applicable law or regulation, the terms of this Agreement.

- **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.

- **Contractor Software** means software, including APIs, and all associated written and electronic documentation and data owned by Contractor and licensed by Contractor to Purchasing Entity. Contractor Software does not include software that is not furnished to Purchasing Entity.

- **Customer Personal Data** means information that identifies an individual that Purchasing Entity directly or indirectly makes accessible to Contractor and that Contractor collects, holds or uses in the course of providing the Services.

- **Cutover** means the date Purchasing Entity's obligation to pay for Services begins.

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

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

- **Data Categorization** means a Purchasing Entity's designation of Data as High Risk Data, Moderate Risk Data, or Low Risk Data under the Agreement. Any Data not expressly designated by a Purchasing Entity will be considered Low Risk Data under the Agreement.

- **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 Purchasing Entities directly for such Services. Contactor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the term of the corresponding Participating Addendum. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

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

- **Infrastructure as a Service (IaaS)** as used in this Master Agreement is defined as the capability provided to the Purchasing Entity to provision processing, storage, networks, and other fundamental computing resources where the Purchasing Entity is able to deploy and run arbitrary software, which can include operating systems and applications. The Purchasing Entity does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

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

- **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** has the definition set forth in §1(A) above.

- **Minimum Payment Period** means the Minimum Payment Period identified for a Service Component in a Pricing Schedule or Service Guide during which Purchasing Entity is required to pay recurring charges for the Service Component.

- **Minimum Retention Period** means the Minimum Retention Period identified for a Service Component in a Pricing Schedule or Service Guide during which Purchasing Entity is required to maintain service to avoid the payment (or repayment) of certain credits, waived charges or amortized charges.

- **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 designated as High Risk Data or Moderate Risk Data 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 (A) provisions required under the laws of the corresponding State; and/or (B) provisions mutually agreed upon between such Participating Entity and Contractor.

- **Participating Entity** means a Participating State or other authorized entity that has properly executed a Participating Addendum.

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

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

- **Platform as a Service (PaaS)** as used in this Master Agreement is defined as the capability provided to the Purchasing Entity to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The Purchasing Entity 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.

- **Pricing Schedule** means a pricing schedule (including related attachments) or other document that (A) is attached to or is later executed by a Participating Entity; (B) that includes supplemental information relating to the corresponding Services (including links to an applicable Service Guide); and (C) references this Master Agreement.

- **Pricing Schedule Effective Date** of a Pricing Schedule means the date on which the last party signs the Pricing Schedule unless a later date is required by regulation or law.

- **Pricing Schedule Term** means the term of an individual Pricing Schedule, if applicable.

- **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 (A) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (B) 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 (1) that identifies the individual; or (2) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. The term "Individually Identifiable Health Information shall have the same meaning as the term is given in 45 C.F.R.

§160.103.

- **Purchased Equipment** means equipment or other tangible products Purchasing Entity purchases under this Agreement, including any replacements of Purchased Equipment provided to Purchasing Entity. Purchased Equipment also includes any internal code required to operate such Equipment. Purchased Equipment does not include Software but does include any physical media provided to Purchasing Entity on which Software is stored.

- **Purchasing Entity** means (A) a Participating Entity; and/or (B) 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 that issues a purchase order against the corresponding Participating Addendum and the Master Agreement.

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

- **Services** means all products and services AT&T provides pursuant to the Agreement.

- **Service Component** means an individual component of a Service provided under the Master Agreement.

- **Service Guides** means (A) an AT&T dynamic, online document that includes the descriptions, pricing and other terms and conditions for a Service which can be found at www.att.com/servicepublications through a link in the Services' Pricing Schedule, or other locations Contractor may designate; and (B) the AUP.

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

- **Site** means a physical location, including Purchasing Entity's collocation space on Contractor's or its Affiliate's or subcontractor's property, where Contractor installs or provides a Service.

- **Software** means Contractor Software and Vendor Software.

- **Software as a Service (SaaS)** as used in this Master Agreement is defined as the capability provided to the Participating Entity 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 Participating Entity 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 under solicitation #CH16012 by the State of Utah, as the Lead State, to obtain Contractor's response thereto.

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

- **Subcontractor** means any person or third party entity with whom Contractor contracts specifically tailored to meet the Purchasing Entity's needs and dedicated exclusively to the performance of all or a portion of the Services hereunder. For avoidance of doubt, suppliers, manufacturers, and providers of off-the-shelf, commercially-available goods or services shall not be deemed Subcontractors.

- **Third-Party Service** means a service provided directly to Purchasing Entity by a third party under a separate agreement between Purchasing Entity and the third party.

- **User** means anyone who uses or accesses any Service provided to Purchasing Entity. Purchasing Entity will cause Users to comply with this Agreement and is responsible for Users' use of any Service unless expressly provided to the contrary in an applicable Service Guide.

- **Vendor Software** means software, including APIs, and all associated written and electronic documentation and data Contractor furnishes to Purchasing Entity, other than Contractor Software.

3. TERM OF THE MASTER AGREEMENT: The initial term of this Master Agreement is for ten (10) years with no renewal options.

(A) Service Discontinuance. Notwithstanding the foregoing, and unless applicable law or regulation mandates otherwise, Contractor may discontinue providing a Service upon twelve (12) months' notice, or a Service Component upon one hundred twenty (120) days' notice, but only where Contractor generally discontinues providing the Service or Service Component to similarly–situated customers.

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

5. ASSIGNMENT AND SUBCONTRACTING:

(A) Lead State may, without Contractor's consent but upon notice to Contractor, assign in whole or relevant part its rights and obligations under this Master Agreement to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint. Contractor may, without Lead State's consent but upon notice to Lead State, assign in whole or relevant part its rights and obligations under this Master Agreement to a Contractor Affiliate. In no other case may this Master Agreement be assigned by either party without the prior written consent of the other party (which consent will not be unreasonably withheld or delayed). In the case of any assignment, the assigning party shall remain financially responsible for the performance of the assigned obligations.

(B) Contractor may subcontract to an Affiliate or a third party work to be performed under this Master Agreement but will remain financially responsible for the performance of such obligations.

(C) In countries where Contractor does not have an Affiliate to provide a Service, Contractor may assign its rights and obligations related to such Service to a local service provider, but Contractor will remain responsible to Purchasing Entity for such obligations. In certain countries, Purchasing Entity may be required to contract directly with the local service provider.

6. DISCOUNT GUARANTEE PERIOD: Contractor guarantees the pricing and discounts set forth in the Master Agreement for the entire term of the Master Agreement. Contractor may decrease a Service's net price through an individual order or Participating Addendum, and such decrease does not obligate Contractor to decrease a Service's net price to another Purchasing Entity or otherwise decrease the Service's net price as set forth in the Master Agreement.

7. LIMITATIONS OF LIABILITY AND DISCLAIMERS

(A) Limitation of Liability. For purposes of this §7 only, the term "Party," means the Lead State, the Participating Entity, and/or the Purchasing Entity on the one hand, and means AT&T on the other.

(1) EITHER PARTY'S ENTIRE LIABILITY AND THE OTHER PARTY'S EXCLUSIVE REMEDY FOR DAMAGES ON ACCOUNT OF ANY CLAIM ARISING OUT OF AND NOT DISCLAIMED UNDER THIS AGREEMENT SHALL BE:

(a) FOR BODILY INJURY, DEATH OR DAMAGE TO REAL PROPERTY OR TO TANGIBLE PERSONAL PROPERTY PROXIMATELY CAUSED BY A PARTY'S NEGLIGENCE, PROVEN DIRECT DAMAGES;

(b) FOR BREACH OF §8 (Confidential Information), PROVEN DIRECT DAMAGES;

(c) FOR ANY THIRD-PARTY CLAIMS, THE REMEDIES AVAILABLE UNDER §13 (Third Party Claims);

(d) FOR CLAIMS ARISING FROM THE OTHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, PROVEN DAMAGES; OR

(e) FOR CLAIMS OTHER THAN THOSE SET FORTH IN §7(A)(1)(a)-(d), PROVEN DIRECT DAMAGES NOT TO EXCEED, ON AN AGGREGATE BASIS DURING ANY TWELVE (12) MONTH PERIOD, AN AMOUNT EQUAL TO TWO TIMES THE TOTAL NET CHARGES INCURRED BY A PURCHASING ENTITY DURING THAT TWELVE (12) MONTH TIME-PERIOD UNDER A CORRESPONDING PARTICIPATING ADDENDUM OR $3,000,000.00, WHICHEVER IS GREATER.

(2) EXCEPT AS SET FORTH IN §13 (Third Party Claims) OR IN THE CASE OF A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES OR FOR INCREASED COST OF OPERATIONS.

(3) THE LIMITATIONS IN THIS §7 SHALL NOT LIMIT PURCHASING ENTITY'S RESPONSIBILITY FOR THE PAYMENT OF ALL PROPERLY DUE CHARGES UNDER THIS AGREEMENT.

(B) Disclaimer of Liability. CONTRACTOR WILL NOT BE LIABLE FOR ANY DAMAGES ARISING OUT OF OR RELATING TO: INTEROPERABILITY, ACCESS OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, DATA, EQUIPMENT, SERVICES, CONTENT OR NETWORKS PROVIDED BY PURCHASING ENTITY OR THIRD PARTIES; SERVICE DEFECTS, SERVICE LEVELS, DELAYS OR ANY SERVICE ERROR OR INTERRUPTION, INCLUDING INTERRUPTIONS OR ERRORS IN ROUTING OR COMPLETING ANY 911 OR OTHER EMERGENCY RESPONSE CALLS OR ANY OTHER CALLS OR TRANSMISSIONS (EXCEPT FOR CREDITS EXPLICITLY SET FORTH IN THIS AGREEMENT); LOST OR ALTERED MESSAGES OR TRANSMISSIONS; OR UNAUTHORIZED ACCESS TO OR THEFT, ALTERATION, LOSS OR DESTRUCTION OF PURCHASING ENTITY'S (OR ITS AFFILIATES', USERS' OR THIRD PARTIES') APPLICATIONS, CONTENT, DATA, PROGRAMS, INFORMATION, NETWORKS OR SYSTEMS.

(1) Notwithstanding the foregoing, the disclaimers in §7(B) remain subject to all applicable Service Level Agreements, and the Data Security Addendum set forth in Attachment B.

8. CONFIDENTIALITY, NON-DISCLOSURE, AND INJUNCTIVE RELIEF

(A) Obligations. A disclosing party's Confidential Information will: (1) not be disclosed, except to the receiving party's employees, agents and contractors having a need-to-know (but only if such agents and contractors are not direct competitors of the other party and agree in writing to use and disclosure restrictions as restrictive as this §8 or to the extent authorized to be revealed by law, governmental authority or legal process (but only if such disclosure is limited to that which is so authorized and prompt

notice is provided to the disclosing party to the extent practicable and not prohibited by law, governmental authority or legal process); (2) be held in confidence; and (3) be used only for purposes of using the Services, evaluating proposals for new services or performing this Agreement (including in the case of Contractor to detect fraud, to check quality and to operate, maintain and enhance the network and Services).

(B) Exceptions. The restrictions in this §8 will not apply to any information that: (1) is independently developed by the receiving party without use of the disclosing party's Confidential Information; (2) is lawfully received by the receiving party free of any obligation to keep it confidential; (3) becomes generally available to the public other than by breach of this Agreement; or (4) is compelled disclosed by subpoena, or order of a court of competent jurisdiction.

(C) Privacy. Each party is responsible for complying with the privacy laws applicable to its business. Contractor shall require its personnel, agents and contractors around the world who process Purchasing Entity Personal Data to protect Purchasing Entity Personal Data in accordance with the data protection laws and regulations applicable to Contractor's business. If Purchasing Entity does not want Contractor to comprehend Purchasing Entity data to which it may have access in performing Services, Purchasing Entity must encrypt such data so that it will be unintelligible. Purchasing Entity is responsible for obtaining consent from and giving notice to its end users, employees and agents regarding Purchasing Entity's and Contractor's collection and use of the end user, employee or agent information in connection with a Service. Purchasing Entity will only make accessible or provide Lead State Personal Data to Contractor when it has the legal authority to do so. Unless otherwise directed by Purchasing Entity in writing, if Contractor designates a dedicated account representative as Purchasing Entity's primary contact with Contractor, Purchasing Entity authorizes that representative to discuss and disclose Purchasing Entity's customer proprietary network information to any employee or agent of Purchasing Entity without a need for further authentication or authorization.

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

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

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position or Lead State'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 subject to notice and Contractor's ability to cure pursuant to §10.

10. DEFAULTS, TERMINATION, SUSPENSION, AND REMEDIES:

(A) Default.

(1) The occurrence of any of the following events shall be an event of default (an "Event of Default") under this Master Agreement or Participating Addendum, as applicable:

(a) Nonperformance of contractual requirements; or

(b) A material breach of any term or condition of the Agreement; or

(c) 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

(d) 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; or

(e) Any default specified in another section of the Agreement.

(2) Upon the occurrence of an Event of Default under the Master Agreement and/or a Participating Addendum, the non-defaulting party 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 non-defaulting party shall not be required to provide advance written notice or a cure period and may immediately terminate the Master Agreement or Participating Addendum (as applicable) in whole or in part if the non-defaulting party, 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 the defaulting party's liability for damages.

(3) 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, then defaulting party shall be in breach of its obligations under this Master Agreement and/or the Participating Addendum (as applicable), and the non-defaulting party shall have the right to exercise any or all of the following remedies:

(a) Exercise any remedy provided by law; and

(b) Terminate this Master Agreement and any applicable Participating Addenda or portions thereof; and

(c) Suspend Contractor's performance; and

(d) Withhold payment of only those charges associated with the affected services until the default is remedied.

(4) Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, the non-defaulting party 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. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a non-defaulting party under the applicable commercial code.

(B) Termination/Suspension.

(1) This Agreement may be terminated immediately upon notice by either party if the other party becomes insolvent, ceases operations, is the subject of a bankruptcy petition, enters receivership or any state insolvency proceeding or makes an assignment for the benefit of its creditors.

(2) The following additional termination and/or suspension provisions apply:

(a) Material Breach. If either party commits and Event of Default (see §10(A)(1)) fails to perform or observe any material warranty, representation, term or condition of this Agreement, including non-payment of charges, and such failure continues un-remedied for thirty (30) days after receipt of notice, the aggrieved party may terminate (and Contractor may suspend and later terminate) the affected Service Components and, if the breach materially and adversely affects the entire Agreement, terminate (and Contractor may suspend and later terminate) the entire Agreement.

(b) Materially Adverse Impact. If Contractor revises a Service Guide, the revision has a materially adverse impact on Participating Entity and Contractor does not affect revisions that remedy such materially adverse impact within thirty (30) days after receipt of notice from Participating Entity, then Participating Entity may, as Participating Entity's sole remedy, elect to terminate the affected Service Components on thirty (30) days' notice to Contractor, given not later than ninety (90) days after Participating Entity first learns of the revision to the Service Guide. "Materially adverse impacts" do not include changes to non-stabilized pricing, changes required by governmental authority, or assessment of or changes to additional charges such as surcharges or taxes.

(c) Internet Services. If Participating Entity fails to rectify a violation of the AUP within fifteen (15) days after receiving notice from Contractor, Contractor may suspend the affected Service Components. Contractor reserves the right, however, to suspend or terminate immediately when: (i) Contractor's suspension or termination is in response to multiple or repeated AUP violations or complaints; (ii) Contractor is acting in response to a court order or governmental notice that certain conduct must be stopped; or (iii) Contractor reasonably determines that (x) it may be exposed to sanctions, liability, prosecution or other adverse consequences under

applicable law if Contractor were to allow the violation to continue; (y) such violation may harm or interfere with the integrity, normal operations or security of Contractor's network or networks with which Contractor is interconnected or may interfere with another customer's use of Contractor services or the Internet; or (z) such violation otherwise presents an imminent risk of harm to Contractor, Contractor's customers or its or their respective employees.

(d) Fraud or Abuse. Contractor may terminate or suspend an affected Service or Service Component if a corresponding Purchasing Entity, in the course of breaching the Agreement: (i) commits a fraud upon Contractor; (ii) uses the Service to commit a fraud upon another party; (iii) unlawfully uses the Service; (iv) abuses or misuses Contractor's network or Service; or (v) interferes with another customer's use of Contractor's network or services.

(e) Infringing Services. If the options described in §13 are not reasonably available, Contractor may at its option terminate the affected Services or Service Components without liability other than as stated in §13.

(f) Hazardous Materials. If Contractor encounters any Hazardous Materials at the Site, Contractor may terminate the affected Services or Service Components or may suspend performance until Purchasing Entity removes and remediates the Hazardous Materials at Purchasing Entity's expense in accordance with applicable law.

(g) Non-Appropriations of Funding. If Purchasing Entity is a government entity dependent on government funding, by participating in this Agreement, Purchasing Entity agrees that Purchasing Entity has funds appropriated and available to pay all amounts due hereunder through the end of Purchasing Entity's current fiscal period. Purchasing Entity further agrees to use reasonable efforts to obtain all appropriations and funding necessary to pay for the Services for each subsequent fiscal period through the end of the applicable Minimum Payment Period. In the event Purchasing Entity is unable to obtain the necessary appropriations or funding for the Services provided under this Agreement, Purchasing Entity may terminate the Services without liability for the Termination Charges set forth in §10 (Defaults, Termination, Suspension, and Remedies) upon the following conditions: (i) Purchasing Entity has taken appropriate actions necessary to obtain adequate appropriations or funding; and (ii) despite Purchasing Entity's best efforts funds have not been appropriated and are otherwise unavailable to pay for the Services. Purchasing Entity must provide Contractor thirty (30) days' written notice of its intent to terminate the Services under this section. Termination of the Services for failure to obtain necessary appropriations or funding shall be effective as of the last day for which funds were appropriated or otherwise made available. If Purchasing Entity terminates the Services under this Agreement under this section, Purchasing Entity agrees as follows: (X) it will pay all amounts due for Services incurred through date of termination, and reimburse all unrecovered non-recurring charges; and (Y) it will not contract with any other provider for the same or substantially similar services or equipment for the immediately subsequent, non-funded, fiscal year.

(h) This Master Agreement may be terminated by either the Lead State or Contractor upon sixty (60) days' written notice prior to the effective date of the

termination. Termination may be in whole or in part. Further, Contracting and a Participating Entity may, but are not required to, negotiate mutually acceptable termination for convenience language in their corresponding Participating Addendum.

(i) Any termination under this §10 shall not affect the rights and obligations attending orders outstanding 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's Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

(C) Effect of Termination.

(1) Termination or suspension by either party of a Service or Service Component does not waive any other rights or remedies a party may have under this Agreement and will not affect the rights and obligations of the parties regarding any other Service or Service Component.

(2) If a Service or Service Component is terminated, Purchasing Entity will pay all amounts incurred prior to the effective date of termination.

(D) Termination Charges.

(1) If Lead State terminates this Agreement or an affected Service or Service Component for cause, or for non-appropriation (under §10(B)(2)(g)) in accordance with the Agreement then Lead State will not be liable for termination charges.

(2) If a Participating Entity terminates its PA or an affected Service or Service Component for cause or for non-appropriation (under §10(B)(2)(g)) in accordance with the Agreement, then that Participating Entity and its corresponding Purchasing Entities will not be liable for termination charges.

(3) If a Purchasing Entity terminates an affected Service or Service Component for cause or for non-appropriation (under §10(B)(2)(g)) in accordance with the Agreement, then Purchasing Entity will not be liable for termination charges.

(4) If Contractor terminates, or an affected Service or Service Component for cause, then the corresponding Participating Entity or Purchasing Entity (as applicable depending on which entity is financially responsible for the affected Service or Service Component), is liable for termination charges.

(5) If Purchasing Entity or Contractor terminates a Service or Service Component prior to Cutover for cause, then Purchasing Entity (a) will pay any pre-Cutover termination or cancellation charges set out in a Pricing Schedule or Service Guide, or (b) in the absence of such specified charges, will reimburse Contractor for time and materials incurred prior to the effective date of termination, plus any third party charges resulting from the termination.

(6) If Purchasing Entity or Contractor terminates a Service or Service Component after Cutover for cause, then Purchasing Entity will pay applicable termination charges as follows: (a) 50% (unless a different amount is specified in the Pricing Schedule) of any unpaid recurring charges for the terminated Service or Service Component attributable to the unexpired portion of an applicable Minimum Payment Period; (b) if termination occurs before the end of an applicable Minimum Retention Period, any associated credits or waived or unpaid non-recurring charges; and (c) any charges incurred by Contractor from a third party (i.e., not a Contractor Affiliate) due to the termination. The charges set forth in §§10(B)(6)(a) and (b) will not apply if a terminated Service Component is replaced with an upgraded Service Component at the same Site, but only if the Minimum Payment Period or Minimum Retention Period, as applicable, (the "Minimum Period") and associated charge for the replacement Service Component are equal to or greater than the corresponding Minimum Period and associated charge for the terminated Service Component, respectively, and if the upgrade is not restricted in the applicable Service Guide.

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

12. FORCE MAJEURE. Neither party will be liable for any delay, failure in performance, loss or damage due to fire, explosion, cable cuts, power blackout, earthquake, flood, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism, acts of God, acts of a public enemy, acts or omissions of carriers or suppliers, acts of regulatory or governmental agencies or other causes beyond such party's reasonable control.

13. THIRD PARTY CLAIMS.

(A) Contractor's Obligations. Contractor agrees at its expense to defend and either to settle any third-party claim against Lead State, Participating Entities, Purchasing Entities, or their Affiliates and their respective employees and directors or to pay all damages that a court finally awards against such parties for a claim alleging that a Service provided to a Purchasing Entity under this Agreement infringes any patent, trademark, copyright or trade secret, but not where the claimed infringement arises out of or results from: (1) Lead State's, Participating Entity's, Purchasing Entities, or their Affiliate's or a User's content; (2) modifications to the Service by a Purchasing Entity, its Affiliate or a third party, or combinations of the Service with any non-Contractor services or products by Purchasing Entity or others; (3) Contractor's adherence to Lead State's, Participating Entity's, Purchasing Entity's, or their Affiliate's written requirements; or (4) use of a Service in violation of this Agreement.

(B) Infringing Services. Whenever Contractor is liable under §13, Contractor may at its option either procure the right for Purchasing Entity to continue using, or may replace or modify, the Service so that it is non-infringing.

(C) Notice and Cooperation. The party seeking defense or settlement of a third-party claim under this §13 will provide notice to the other party promptly upon learning of any claim for which defense or settlement may be sought, but failure to do so will have no effect except to the extent the other party is prejudiced by the delay. The party seeking defense or settlement will allow the other party to control the defense and settlement of the claim and will reasonably cooperate with the defense. The defending party will use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim where relief against the party being defended is limited to monetary damages that are paid by the defending party under this §13.

(D) Limitations. Contractor's obligations under §13 shall not extend to actual or alleged infringement or misappropriation of intellectual property based on Purchased Equipment, Software, or Third-Party Services.

14. INDEPENDENT CONTRACTOR: Each party is an independent contractor. Neither party controls the other, and neither party nor its Affiliates, employees, agents or contractors are Affiliates, employees, agents or contractors of the other party.

15. 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 provided in the 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.

16. INSURANCE

(A) Requirement. 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 eligible 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) Minimum Acceptable Limits. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual

liability, personal injury (including death), advertising liability, and property damage, with a limit of $1million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Professional Liability Insurance Inclusive of Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Insurance Coverage per claim or wrongful act and in the aggregate
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(2) Contractor must comply with any applicable State Workers Compensation Employers Liability Insurance Requirements.

(C) Premiums. Contractor shall pay premiums on all insurance policies. Contractor will provide the Lead State at least thirty (30) calendar days' prior written notice of cancellation of any required coverage that is not replaced.

(D) Evidence of Insurance. Prior to commencement of performance, Contractor shall provide to the Lead State a certificate of insurance evidencing the Contractor's general liability insurance policy to the Lead State that (1) includes the Participating States identified in the Request for Proposal as additional insureds, (2) provides that the Contractor's required liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

(1) Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability. 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.

(E) Coverage No Limit on Liability. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

(F) Self-Insurance. Contractor may self-insure any of the required coverage as long as it or its affiliated parent maintains a new worth of at least $200,000,000 as shown in certified financials.

17. LAWS AND REGULATIONS: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. 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.

19. ORDERING

(A) Agreement Numbers on Labels. Master Agreement number and initial purchase order numbers shall be clearly shown on all shipping labels, packing slips, and invoices.

(B) Project-Specific Requirements. 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.

(C) Procedures. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

(D) Participating Addendum Requirement. Contractor shall not begin providing Services without an appropriate Participating Addendum compliant with the law of the Purchasing Entity.

(E) Placement. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

(F) Requirement. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

(G) Communications. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

(H) Timing and Performance. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement, as subject to the non-appropriation language in §10(B)(2)(g) herein. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination.

(1) The respective obligations of Lead State, Participating Entities, Purchasing Entities, and Contractor that by their nature would continue beyond the termination or expiration of this Agreement, including the obligations set forth in §8 (Confidential Information), §7 (Limitations of Liability and Disclaimers) and §13 (Third Party Claims), will survive such termination or expiration.

20. PARTICIPANTS AND SCOPE

(A) Participating Addendum Required. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the

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

(B) State Chief Procurement Official Approval. Subject to §20(C) herein 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.

(1) Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[1].

(C) Financial Obligations. 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 Entities are limited to the orders placed by the departments or other state agencies and institutions are subject to §19 herein. Participating Entities incur no financial obligations on behalf of political subdivisions.

(D) NASPO ValuePoint not a Party. 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.

(E) Participating Addenda' Effect on Master Agreement. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

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

(F) Non-State Participating Entities. Participating Entities who are not states may 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. The Participating Entity must coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; the Participating Entity must ensure that it has the requisite procurement authority to execute a Participating Addendum.

(G) Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. PRICING AND BILLING:

(A) Pricing and Pricing Schedule Term; Terms Applicable After End of Pricing Schedule Term. The prices listed in a Pricing Schedule are stabilized until the end of the Pricing Schedule Term and will apply in lieu of the corresponding prices set forth in the applicable Service Guide. No promotion, credit, discount or waiver set forth in a Service Guide will apply. Unless the Pricing Schedule states otherwise, at the end of the Pricing Schedule Term, Purchasing Entity may continue Service (subject to any applicable notice or other requirements in a Service Guide for Purchasing Entity to terminate a Service Component) under a month-to-month service arrangement at the prices, terms and conditions in effect on the last day of the Pricing Schedule Term. Contractor may change such prices, terms or conditions on thirty (30) days' prior notice to Purchasing Entity.

(B) Additional Charges and Taxes. Prices set forth in a Pricing Schedule are exclusive of and Purchasing Entity will pay all taxes (excluding those on Contractor's net income), surcharges, recovery fees, customs clearances, duties, levies, shipping charges and other similar charges (and any associated interest and penalties resulting from Purchasing Entity's failure to timely pay such taxes or similar charges) relating to the sale, transfer of ownership, installation, license, use or provision of the Services, except to the extent Purchasing Entity provides a valid exemption certificate prior to the delivery of Services. To the extent required by law, Purchasing Entity may withhold or deduct any applicable taxes from payments due to Contractor, provided that Purchasing Entity will use reasonable commercial efforts to minimize any such taxes to the extent allowed by law or treaty and will furnish Contractor with such evidence as may be required by relevant taxing authorities to establish that such tax has been paid so that Contractor may claim any applicable credit.

(C) Billing. Unless a Service Guide specifies otherwise, Purchasing Entity's obligation to pay for a Service Component begins upon availability of the

Service Component to Purchasing Entity. Purchasing Entity will pay Contractor without deduction, setoff or delay for any reason (except for withholding taxes as provided in §21(B) - Additional Charges and Taxes or in §21(E) - Delayed Billing; Disputed Charges). At Purchasing Entity's request, but subject to Contractor's consent (which may not be unreasonably withheld or withdrawn), Purchasing Entity's Affiliates may be invoiced separately, and Contractor will accept payment from such Affiliates. Purchasing Entity will be responsible for payment if Purchasing Entity's Affiliates do not pay charges in accordance with this Agreement. Contractor may require Purchasing Entity or its Affiliates to tender a deposit if Contractor determines, in its reasonable judgment, that Purchasing Entity or its Affiliates are not creditworthy, and Contractor may apply such deposit to any charges owed.

(D) Payments. Payment is due within thirty (30) days after the date of the invoice and must refer to the invoice number. Charges must be paid in the currency specified in the invoice. Restrictive endorsements or other statements on checks are void. Purchasing Entity will reimburse Contractor for all costs associated with collecting delinquent or dishonored payments, including reasonable attorneys' fees. Contractor may charge late payment fees at the lowest of (1) 1.5% per month (18% per annum), or (2) the maximum rate allowed by law for overdue payments.

(E) Delayed Billing; Disputed Charges. Purchasing Entity will not be required to pay charges for Services initially invoiced more than six (6) months after close of the billing period in which the charges were incurred. If Purchasing Entity disputes a charge, Purchasing Entity will provide notice to Contractor specifically identifying the charge and the reason it is disputed within 6 months after the date of the invoice in which the disputed charge initially appears, or Purchasing Entity waives the right to dispute the charge. The portion of charges in dispute may be withheld and will not be considered overdue until Contractor completes its investigation of the dispute, but Purchasing Entity may incur late payment fees in accordance with §21(D) (Payments). Following Contractor's notice of the results of its investigation to Purchasing Entity, payment of all properly due charges and properly accrued late payment fees must be made within ten (10) business days of the investigation's conclusion, or the original thirty (30) day payment period plus ten (10) business days, whichever is later. Contractor will reverse any late payment fees that were invoiced in error.

(F) Credit Terms. Contractor retains a lien and purchase money security interest in each item of Purchased Equipment and Vendor Software until Purchasing Entity pays all sums due. Contractor is authorized to sign and file a financing statement to perfect such security interest.

22. [RESERVED]

23. 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 those specified in the Solicitation.

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

25. PURCHASING ENTITY DATA: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata. 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 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. The obligation shall extend beyond the term of this Master Agreement in perpetuity. Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. RECORDS ADMINISTRATION AND AUDIT.

(A) Maintenance Requirement and Lead State's Audit Rights. 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 (1) performance and administration of payments and fees; and/or (2) Contractor's billing for Services rendered under the Agreement. Contractor shall permit the Lead State the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

(B) Remedies. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

(C) Timing. Contractor will agree to allow the Lead State's auditors reasonable access to our records to the extent necessary to verify the accuracy of the Administrative Fees paid to Lead State and Contractor's billing for Services rendered under the Agreement. Contractor will follow applicable legal requirements and its internal record retention policies with respect to records relating to this project. Subject to Contractor's reasonable security requirements and not more than once every twelve (12) months, the Lead State may, at its own expense, review Contractor's relevant records for a period not to exceed the immediately preceding six (6) years, for the purpose of assessing the accuracy of Contractor's Administrative Fee payments and billing for Services rendered under the Agreement. The Lead State may employ such assistance, as it deems desirable to conduct such reviews, but may not employ the

assistance of any entity that derives a substantial portion of its revenues from the provision of services that are substantially similar to the Services provided hereunder or any person who has previously made prohibited use of Contractor's Confidential Information. Lead State will cause any person retained for this purpose to execute a non-disclosure agreement. Such reviews shall take place at a time and place agreed upon by the parties. Lead State's normal internal invoice reconciliation procedures will not be considered a review of Contractor's relevant billing records. Contractor will promptly correct any payment error that is revealed in a billing review, including refunding any underpayment by Contractor.

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

(E) Participating Entities. Contractor and a Participating Entity may, but are not required to, negotiate mutually-acceptable audit language in their corresponding Participating Addendum.

27. ADMINISTRATIVE FEE: The Contractor shall pay to NASPO ValuePoint, or its assignee, an administrative fee of one-quarter of one percent (0.25% or 0.0025) of the total billed charges (after the application of all discounts and credits) which are invoiced to Purchasing Entities (exclusive of taxes, surcharges, and fees) for the Services provided under the Master Agreement (the "NASPO ValuePoint Administrative Fee"). The NASPO ValuePoint Administrative Fee shall be submitted quarterly (no later than sixty (60) days following the end of each calendar quarter.

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

28. SYSTEM FAILURE OR DAMAGE: Contractor is bound by Federal and State regulations for priority restoration of services. The Telecommunications Service Priority (TSP) restoration standard issued by the Federal Government is the only legal mechanism to receive priority provisioning and restoral of telecommunications service in the Contractor regions. Contractor complies with the FCC Telecommunications Service Program and will be happy to work with the Lead State to define restoral processes in alignment with the FCC Telecommunications Service Priority "TSP" policy. To the best of Contractor's ability, Contractor will restore service to the Lead State following normal

process and procedures and will do so as quickly and safely as possible.

29. TITLE TO PRODUCT: All intellectual property in the Services shall be the sole and exclusive property of Contractor or its suppliers, as applicable. Each party shall retain all of its rights in its pre-existing intellectual property.

30. DATA PRIVACY: Each party is responsible for complying with the privacy laws applicable to its business. Contractor shall require its personnel, agents and contractors around the world who process Lead State Personal Data to protect Lead State Personal Data in accordance with the data protection laws and regulations applicable to Contractor's business. If Lead State does not want Contractor to comprehend Lead State data to which it may have access in performing Services, Lead State must encrypt such data so that it will be unintelligible. Lead State is responsible for obtaining consent from and giving notice to its Users, employees and agents regarding Lead State's and Contractor's collection and use of the User, employee or agent information in connection with a Service. Lead State will only make accessible or provide Lead State Personal Data to Contractor when it has the legal authority to do so. Unless otherwise directed by Lead State in writing, if Contractor designates a dedicated account representative as Lead State's primary contact with Contractor, Lead State authorizes that representative to discuss and disclose Lead State's customer proprietary network information to any employee or agent of Lead State without a need for further authentication or authorization.

31. WARRANTY:

(A) Purchased Equipment and Vendor Software Warranty. Contractor shall pass through to Purchasing Entity any warranties for Purchased Equipment and Vendor Software available from the manufacturer or licensor. The manufacturer or licensor, and not Contractor, is responsible for any such warranty terms and commitments. ALL SOFTWARE AND PURCHASED EQUIPMENT IS OTHERWISE PROVIDED TO LEAD STATE ON AN "AS IS" BASIS.

(B) Disclaimer of Warranties. CONTRACTOR MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, SPECIFICALLY DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT AND SPECIFICALLY DISCLAIMS ANY WARRANTY ARISING BY USAGE OF TRADE OR BY COURSE OF DEALING. FURTHER, CONTRACTOR MAKES NO REPRESENTATION OR WARRANTY THAT TELEPHONE CALLS OR OTHER TRANSMISSIONS WILL BE ROUTED OR COMPLETED WITHOUT ERROR OR INTERRUPTION (INCLUDING CALLS TO 911 OR ANY SIMILAR EMERGENCY RESPONSE NUMBER) AND MAKES NO GUARANTEE REGARDING NETWORK SECURITY, THE ENCRYPTION EMPLOYED BY ANY SERVICE, THE INTEGRITY OF ANY DATA THAT IS SENT, BACKED UP, STORED OR SUBJECT TO LOAD BALANCING OR THAT CONTRACTOR'S SECURITY PROCEDURES WILL PREVENT THE LOSS OR ALTERATION OF OR IMPROPER ACCESS TO PURCHASING ENTITY'S DATA AND INFORMATION.

(D) Application and Survival. The disclaimer of warranties and limitations of liability set forth in this Agreement will apply regardless of the form of action, whether in contract, equity, tort, strict liability or otherwise, of whether damages were foreseeable and of whether a party was advised of the possibility of such damages and will apply so as to limit the liability of each party and its Affiliates and their respective employees, directors, subcontractors and suppliers. The limitations of liability and disclaimers set out in this §31 will survive failure of any exclusive remedies provided in this Agreement.

32. TRANSITION ASSISTANCE:

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

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

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

33. WAIVER OF BREACH: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

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 SLA 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) Governing Law for Master Agreement.** 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).

(B) Governing Law of Participating Addenda. 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.

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

(D) Federal Venue. 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.

(E) No Waiver. 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's customers 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 provided customers information regarding the Contractors 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 customer 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. 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

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 day following the end of the calendar quarter (as specified in the reporting tool).

(B) Detailed Sales Data. Contractor shall also report detailed sales data by: (1) Vendor name; (2) Vendor contract number; (3) State; (4) Customer type; (5) Bill-to Name; (6) Bill-to address; (7) Bill-to city; (8) Bill-to zip code; (9) Ship-to name; (10) Ship-to address; (11) Ship-to city; (12) Ship-to zip code; (13) Invoice number; (14) Product description; (15) List price/MSRP; (16) NASPO ValuePoint price; (17) Quantity; and (18) Total Price, as applicable. The report shall be submitted in any form required by the solicitation as agreed to by Contractor. 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, as agreed to by Contractor. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement.

(C) Personal Use. For clarification, no sales are authorized for employees' personal use under the Agreement.

(D) Executive Summary. 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 forty-five (45) days after the conclusion of each calendar quarter.

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

(F) Additional Data. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. Miscellaneous Provisions.

(A) Agreement Language. The language of this Agreement is English. If there is a conflict between this Agreement and any translation, the English version will take precedence.

(B) Contractor Deliverables

(1) Contractor will either provide or arrange to have a Contractor Affiliate provide Services to Purchasing Entity and its Users, subject to the availability and operational limitations of systems, facilities and equipment. Where required, a Contractor Affiliate authorized by the appropriate regulatory authority will be the service provider. If an applicable Service Guide expressly permits placement of an order for a Service under this Master Agreement without the execution of a Pricing Schedule, Purchasing Entity may place such an order using Contractor's standard ordering processes (an "Order"), and upon acceptance by Contractor, the Order shall otherwise be deemed a Pricing Schedule under this Master Agreement for the Service ordered.

(2) Services may be provided using equipment owned by Contractor that is located at the Site ("Contractor Equipment"), but title to the Contractor Equipment will remain with Contractor. Purchasing Entity must provide adequate space and electric power for the Contractor Equipment and keep the Contractor Equipment physically secure and free from liens and encumbrances. Purchasing Entity will bear the risk of loss or damage to the Contractor Equipment (other than ordinary wear and tear), except to the extent caused by Contractor or its agents.

(3) Except as specified in a Participating Addendum or Service Guide, title to and risk of loss of Purchased Equipment shall pass to Purchasing Entity on delivery to the transport carrier for shipment to Purchasing Entity's designated location.

(C) Execution by Affiliates. A Contractor Affiliate or Purchasing Entity Affiliate may sign a Pricing Schedule in its own name, and such Affiliate contract will be a separate but associated contract incorporating the terms of this Agreement. Participating Entity and Contractor will cause their respective Affiliates to comply with any such separate and associated contract.

(D) Import/Export Control. Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under this Agreement (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

(E) Injunctive Relief. Nothing in this Agreement is intended to or should be construed to prohibit a party from seeking preliminary or permanent injunctive relief in appropriate circumstances from a court of competent jurisdiction.

(F) License and Other Terms. Software, Purchased Equipment and Third-Party Services may be provided subject to the terms of a separate license or other agreement between the Purchasing Entity and either the licensor, the third-party service provider or the manufacturer. The Purchasing Entity's execution of the Pricing Schedule for or placement of an Order for Software, Purchased Equipment or Third-Party Services is that Purchasing Entity's agreement to comply with such separate agreement. Unless a Service Guide specifies otherwise, Contractor's sole responsibility

with respect to Third-Party Services is to place a Purchasing Entity's orders for Third-Party Services, except that Contractor may invoice and collect payment from such Purchasing Entity for the Third-Party Services.

(G) Notices. Any required notices under this Agreement shall be in writing and shall be deemed validly delivered if made by hand (in which case delivery will be deemed to have been effected immediately), or by overnight mail (in which case delivery will be deemed to have been effected one (1) business day after the date of mailing), or by first class pre-paid post (in which case delivery will be deemed to have been effected five (5) days after the date of posting), or by facsimile or electronic transmission (in which case delivery will be deemed to have been effected on the day the transmission was sent). Any such notice shall be sent to the office of the recipient set forth on the cover page of this Agreement or to such other office or recipient as designated in writing from time to time.

(H) No Third Party Beneficiaries. This Agreement is for the benefit of Lead State, NASPO ValuePoint, Participating Entities, and Purchasing Entities, and Contractor and does not provide any other third party (including Users) the right to enforce it or to bring an action for any remedy, claim, liability, reimbursement or cause of action or any other right or privilege.

(I) Purchasing Entity's Cooperation

(1) Purchasing Entity will in a timely manner allow Contractor access as reasonably required for the Services to property and equipment that Purchasing Entity controls and will obtain at Purchasing Entity's expense timely access for Contractor as reasonably required for the Services to property controlled by third parties such as Purchasing Entity's landlord. Contractor will coordinate with and obtain Purchasing Entity's consent to enter upon Purchasing Entity's property and premises, which consent shall not be unreasonably withheld. If Purchasing Entity unreasonably refuses such consent, then any applicable Service Level Agreements associated with the corresponding Services will not apply. Access rights mean the right to construct, install, repair, maintain, replace and remove access lines and network facilities and the right to use ancillary equipment space within a building for Purchasing Entity's connection to Contractor's network. Purchasing Entity must provide Contractor timely information and access to Purchasing Entity's facilities and equipment as Contractor reasonably requires for the Services, subject to Purchasing Entity's reasonable security policies. Purchasing Entity will furnish any conduit, holes, wireways, wiring, plans, equipment, space, power/utilities and other items as Contractor reasonably requires for the Services and will obtain any necessary licenses, permits and consents (including easements and rights-of-way). Purchasing Entity will have the Site ready for Contractor to perform its work according to a mutually agreed schedule.

(2) Purchasing Entity will ensure that the location at which Contractor installs, maintains or provides Services is a safe working environment, free of Hazardous Materials and reasonably suitable for the Services. "Hazardous Materials" mean any substance or material capable of posing an unreasonable risk to health, safety or property or whose use, transport, storage, handling, disposal or release is regulated by any law related to pollution, to protection of air, water or soil or to health

and safety. Contractor shall have no obligation to perform work at a location that is not a suitable and safe working environment or to handle, remove or dispose of Hazardous Materials.

(J) Severability. If any portion of this Agreement is found to be invalid or unenforceable or if, applicable law mandates a different interpretation or result, the remaining provisions will remain in effect and the parties will negotiate in good faith to substitute for such invalid, illegal or unenforceable provision a mutually acceptable provision consistent with the original intention of the parties.

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

Exhibit 1

To Attachment A of the Master Agreement: Software-as-a-Service

1. **Privacy:** See Attachment A, §§25, 29, and 30.

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

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

2.2 All data obtained by the Contractor from the Purchasing Entity in the performance of the Agreement shall remain the property of the Purchasing Entity.

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

2.4 Unless otherwise stipulated, the Purchasing Entity is responsible for encrypting any Data for which it desires to limit visibility. Encryption would apply for Data both at rest and in transit. Contractor is responsible for transmitting Data regardless of whether the Data is encrypted or not.

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

3. **Data Location:** AT&T reserves the right to staff its various Cloud Services offers with employees and/or contractors from a variety of locations. That is, the Services are not necessarily supported only by US Citizens.

4. **Security Incident or Data Breach Notification:** See Attachment B of the Master Agreement ("Attachment B"), §§1.1, 1.3, 2(h), and 5.

5. **Personal Data Breach Responsibilities:** See Attachment B, §§1.1; 1.3; 2(h); and 5.

6. **Notification of Legal Requests:** See Attachment B, §§3 and 4.

7. **Termination and Suspension of Service:** See Attachment A, §10.

8. **Background Checks:** See Attachment B, §§1.1-1.5.

9. **Access to Security Logs and Reports:** See Attachment B, §§2(h), and 5.

10. Contract Audit: The Contractor shall allow the Lead State to audit conformance to the Master Agreement terms, pursuant to Attachment A, §26.

11. Data Center Audit: See Attachment B, §§3, and 4.

12. Change Control and Advance Notice: Materially Adverse Impact. If AT&T revises a Service Publication, the revision has a materially adverse impact on Customer and AT&T does not affect revisions that remedy such materially adverse impact within 30 days after receipt of notice from Customer, then Customer may, as Customer's sole remedy, elect to terminate the affected Service Components on 30 days' notice to AT&T, given not later than 90 days after Customer first learns of the revision to the Service Publication. "Materially adverse impacts" do not include changes to non-stabilized pricing, changes required by governmental authority, or assessment of or changes to additional charges such as surcharges or taxes.

13. Security: See Attachment B, §§2(a)-(k), and 3.1.

14. Non-disclosure and Separation of Duties: See Attachment B, §§1.1-1.5, and 2.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity, subject to the technical, operational, contractual, and definitional guidelines and limitations of particular products and services as set forth in the applicable product-specific service descriptions and attachments.

16. Import/Export Control: See Attachment A §43.

17. 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 and for which the Contractor has direct responsibility and full management control. . The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. For each eligible product, the system shall be available as stipulated with the corresponding product description, and the Contractor will provide service as defined in the SLA.

18. Assignment and Subcontracting.

18.1 Customer may, without AT&T's consent but upon notice to AT&T, assign in whole or relevant part its rights and obligations under this Agreement to a Customer Affiliate. AT&T may, without Customer's consent, assign in whole or relevant part its rights and obligations under this Agreement to an AT&T Affiliate. In no other case may this Agreement be assigned by either party without the prior written consent of the other party (which consent will not be unreasonably withheld or delayed). In the case of any assignment, the assigning party shall remain financially responsible for the performance of the assigned obligations.

18.2 AT&T may subcontract to an Affiliate or a third-party work to be performed under this Agreement but will remain financially responsible for the performance of such obligations.

18.3 In countries where AT&T does not have an Affiliate to provide a Service, AT&T may assign its rights and obligations related to such Service to a local service provider, but AT&T will remain responsible to Customer for such obligations. In certain countries, Customer may be required to contract directly with the local service provider.

19. Right to Remove Individuals: AT&T will employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with Customer's operations and use of

telecommunications services, to provide and support Customer's use of the Services in accordance with the terms of AT&T's response to this RFP. AT&T retains the right to manage and deploy its personnel as appropriate from time to time. If Customer requests AT&T to substitute an employee, Customer shall provide such requests in writing, explaining in reasonable detail the reason(s) for the removal request. Any such request shall be for lawful reasons. AT&T will work with the Customer to reach a solution geared to providing Services in compliance with contracted standards.

20. Business Continuity and Disaster Recovery: To the extent that a Participating Entity requires a business continuity and disaster recovery plan to accompany the Services provided by Contractor under the Agreement, Contractor will work with such Participating Entity to develop such a plan. Such plan(s) may require additional costs to the Purchasing Entity.

21. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws.

22. Web Services: See Attachment A §§8(c), and 30.

23. Encryption of Data at Rest: The Contractor shall offer hard drive encryption as an optional service and for an additional fee. Such service shall be consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

24. Subscription Terms: License and Other Terms. Software, Purchased Equipment and Third-Party Services may be provided subject to the terms of a separate license or other agreement between Customer and either the licensor, the third-party service provider or the manufacturer. Customer's execution of the Pricing Schedule for or placement of an Order for Software, Purchased Equipment or Third-Party Services is Customer's agreement to comply with such separate agreement. Unless a Service Publication specifies otherwise, AT&T's sole responsibility with respect to Third-Party Services is to place Customer's orders for Third-Party Services, except that AT&T may invoice and collect payment from Customer for the Third-Party Services.

Exhibit 2

To Attachment A of to the Master Agreement: Platform-as-a-Service

1. Privacy: See Attachment A, §§25, 29, and 30.

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

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

2.2 All data obtained by the Contractor from the Purchasing Entity in the performance of the Agreement shall remain the property of the Purchasing Entity.

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

2.4 Unless otherwise stipulated, the Purchasing Entity is responsible for encrypting any Data for which it desires to limit visibility. Encryption would apply for Data both at rest and in transit. Contractor is responsible for transmitting Data regardless of whether the Data is encrypted or not.

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

3. Data Location: AT&T reserves the right to staff its various Cloud Services offers with employees and/or contractors from a variety of locations. That is, the Services are not necessarily supported only by US Citizens.

4. Security Incident or Data Breach Notification: See Attachment B of the Master Agreement ("Attachment B"), §§1.1, 1.3, 2(h), and 5.

5. Breach Responsibilities: See Attachment B, §§1.1; 1.3; 2(h); and 5.

6. Notification of Legal Requests: See Attachment B, §§3 and 4.

7. Termination and Suspension of Service: See Attachment A, §10.

8. Background Checks: See Attachment B, §§1.1-1.5.

9. Access to Security Logs and Reports: See Attachment B, §§2(h), and 5.

10. Contract Audit: The Contractor shall allow the Lead State to audit conformance to the Master Agreement terms, pursuant to Attachment A, §26.

11. Data Center Audit: See Attachment B, §§3, and 4.

12. Change Control and Advance Notice: Materially Adverse Impact. If AT&T revises a Service Publication, the revision has a materially adverse impact on Customer and AT&T does not affect revisions that remedy such materially adverse impact within 30 days after receipt of notice from Customer, then Customer may, as Customer's sole remedy, elect to terminate the affected Service Components on 30 days' notice to AT&T, given not later than 90 days after Customer first learns of the revision to the Service Publication. "Materially adverse impacts" do not include changes to non-stabilized pricing, changes required by governmental authority, or assessment of or changes to additional charges such as surcharges or taxes.

13. Security: See Attachment B, §§2(a)-(k), and 3.1.

14. Non-disclosure and Separation of Duties: See Attachment B, §§1.1-1.5, and 2.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity, subject to the technical, operational, contractual, and definitional guidelines and limitations of particular products and services as set forth in the applicable product-specific service descriptions and attachments.

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 and for which the Contractor has direct responsibility and full management control. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. For each eligible product, the system shall be available as stipulated with the corresponding product description, and the Contractor will provide service as defined in the SLA.

17. [RESERVED]

18. Assignment and Subcontracting.

18.1 Customer may, without AT&T's consent but upon notice to AT&T, assign in whole or relevant part its rights and obligations under this Agreement to a Customer Affiliate. AT&T may, without Customer's consent, assign in whole or relevant part its rights and obligations under this Agreement to an AT&T Affiliate. In no other case may this Agreement be assigned by either party without the prior written consent of the other party (which consent will not be unreasonably withheld or delayed). In the case of any assignment, the assigning party shall remain financially responsible for the performance of the assigned obligations.

18.2 AT&T may subcontract to an Affiliate or a third-party work to be performed under this Agreement but will remain financially responsible for the performance of such obligations.

18.3 In countries where AT&T does not have an Affiliate to provide a Service, AT&T may assign its rights and obligations related to such Service to a local service provider, but AT&T will remain responsible to Customer for such obligations. In certain countries, Customer may be required to contract directly with the local service provider.

19. Right to Remove Individuals: AT&T will employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with Customer's operations and use of telecommunications services, to provide and support Customer's use of the Services in accordance with the terms of AT&T's response to this RFP. AT&T retains the right to manage and deploy its personnel as appropriate from time to time. If Customer requests AT&T to substitute an employee, Customer shall provide such requests in writing, explaining in reasonable detail the reason(s) for the removal request. Any such request shall be for lawful reasons. AT&T will work with the Customer to reach a solution geared to providing Services in compliance with contracted standards.

20. Business Continuity and Disaster Recovery: To the extent that a Participating Entity requires a business continuity and disaster recovery plan to accompany the Services provided by Contractor under the Agreement, Contractor will work with such Participating Entity to develop such a plan. Such plan(s) may require additional costs to the Purchasing Entity.

21. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws.

22. Web Services: See Attachment A §§8(c), and 30.

23. Encryption of Data at Rest: The Contractor shall offer hard drive encryption as an optional service and for an additional fee. Such service shall be consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

24. Subscription Terms: License and Other Terms. Software, Purchased Equipment and Third-Party Services may be provided subject to the terms of a separate license or other agreement between Customer and either the licensor, the third-party service provider or the manufacturer. Customer's execution of the Pricing Schedule for or placement of an Order for Software, Purchased Equipment or Third-Party Services is Customer's agreement to comply with such separate agreement. Unless a Service Publication specifies otherwise, AT&T's sole responsibility with respect to Third-Party Services is to place Customer's orders for Third-Party Services, except that AT&T may invoice and collect payment from Customer for the Third-Party Services.

Exhibit 3

To Attachment A of the Master Agreement: Infrastructure-as-a-Service

1. Privacy: See Attachment A, §§25, 29, and 30.

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

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

2.2 All data obtained by the Contractor from the Purchasing Entity in the performance of the Agreement shall remain the property of the Purchasing Entity.

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

2.4 Unless otherwise stipulated, the Purchasing Entity is responsible for encrypting any Data for which it desires to limit visibility. Encryption would apply for Data both at rest and in transit. Contractor is responsible for transmitting Data regardless of whether the Data is encrypted or not.

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

3. Data Location: AT&T reserves the right to staff its various Cloud Services offers with employees and/or contractors from a variety of locations. That is, the Services are not necessarily supported only by US Citizens.

4. Security Incident or Data Breach Notification: See Attachment B of the Master Agreement ("Attachment B"), §§1.1, 1.3, 2(h), and 5.

5. Breach Responsibilities: See Attachment B, §§1.1; 1.3; 2(h); and 5.

6. Notification of Legal Requests: See Attachment B, §§3 and 4.

7. Termination and Suspension of Service: See Attachment A, §10.

8. Background Checks: See Attachment B, §§1.1-1.5.

9. Access to Security Logs and Reports: See Attachment B, §§2(h), and 5.

10. Contract Audit: The Contractor shall allow the Lead State to audit conformance to the Master Agreement terms, pursuant to Attachment A, §26.

11. Data Center Audit: See Attachment B, §§3, and 4.

12. Change Control and Advance Notice: Materially Adverse Impact. If AT&T revises a Service Publication, the revision has a materially adverse impact on Customer and AT&T does not affect revisions that remedy such materially adverse impact within 30 days after receipt of notice from Customer, then Customer may, as Customer's sole remedy, elect to terminate the affected Service Components on 30 days' notice to AT&T, given not later than 90 days after Customer first learns of the revision to the Service Publication. "Materially adverse impacts" do not include changes to non-stabilized pricing, changes required by governmental authority, or assessment of or changes to additional charges such as surcharges or taxes.

13. Security: See Attachment B, §§2(a)-(k), and 3.1.

14. Non-disclosure and Separation of Duties: See Attachment B, §§1.1-1.5, and 2.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity, subject to the technical, operational, contractual, and definitional guidelines and limitations of particular products and services as set forth in the applicable product-specific service descriptions and attachments.

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 and for which the Contractor has direct responsibility and full management control. . The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. For each eligible product, the system shall be available as stipulated with the corresponding product description, and the Contractor will provide service as defined in the SLA.

17. [RESERVED]

18. Business Continuity and Disaster Recovery: To the extent that a Participating Entity requires a business continuity and disaster recovery plan to accompany the Services provided by Contractor under the Agreement, Contractor will work with such Participating Entity to develop such a plan. Such plan(s) may require additional costs to the Purchasing Entity.

19. Subscription Terms: License and Other Terms. Software, Purchased Equipment and Third-Party Services may be provided subject to the terms of a separate license or other agreement between Customer and either the licensor, the third-party service provider or the manufacturer. Customer's execution of the Pricing Schedule for or placement of an Order for Software, Purchased Equipment or Third-Party Services is Customer's agreement to comply with such separate agreement. Unless a Service Publication specifies otherwise, AT&T's sole responsibility with respect to Third-Party Services is to place Customer's orders for Third-Party Services, except that AT&T may invoice and collect payment from Customer for the Third-Party Services.

ATTACHMENT B

DATA SECURITY ADDENDUM

1. Data Security - General

1.1. Neither AT&T nor Customer represents or guarantees that security procedures will prevent the loss of, alteration of, or improper access to data in its possession or under its management, but each party will comply with this Attachment B concerning measures taken: (i) by Customer to encrypt data prior to transmission or storage via the Services; and (ii) by AT&T to safeguard data in transit on an AT&T network or stored by Customer on AT&T servers.

1.2. AT&T will maintain programs and processes under which employees, contractors, and subcontractors are screened, trained on security policies and made aware of their responsibilities with regard to AT&T and Customer's data. AT&T will also maintain a comprehensive security program with the objective of broadly incorporating security measures into all AT&T's computing and networking environments ("AT&T Security Program").

1.3. AT&T will maintain a set of security standards drawing upon leading industry standards (e.g., ISO/IEC 27001:2005, etc.). In providing Services under the Agreement, AT&T will observe AT&T security standards.

1.4. AT&T will regularly re-evaluate and modify its security standards at its discretion as generally accepted industry standards evolve, as new technologies emerge or as new threats are identified. AT&T's security standards are themselves sensitive information and as part of the AT&T Security Program the standards are kept confidential and generally not disclosed to third parties.

1.5. The parties acknowledge that Services offered by AT&T have varying levels of inherent security risk. In addition, some Services may involve the transmission or storage of voice and data traffic from, to, on or over third-party networks or facilities which may not have the same protections against unauthorized access that AT&T employs.

2. AT&T Information and Network Security Customer Reference Guide/AT&T Security Program

2.1. AT&T has provided Customer with a copy of the *AT&T Information & Network Security Customer Reference Guide (March, 2017, V5),* which provides an overview of the AT&T Security Program as of the publication date. AT&T anticipates that the AT&T Security Program will continuously evolve, and AT&T therefore has advised Customer that the policies and procedures described in the *AT&T Information & Network Security Customer Reference Guide* may be changed by AT&T without notice to or consultation with Customer. Upon request AT&T will provide a then-current copy of the *AT&T Information & Network Security Customer Reference Guide* to Customer.

2.2. AT&T employs a broad spectrum of security tools and methods in the AT&T Security Program. Following are some of the tools and methods used by AT&T in one or more aspects of the program as of the Master Agreement's effective date. Although the tools and methods will evolve over time, the current description provides a general indication of the depth and scope of the AT&T Security Program.

(a) **Security Policy** – AT&T security standards are formally reviewed, approved, published, and communicated to employees and relevant parties responsible for supporting AT&T's business operations and services. AT&T has established security standards that, in combination with other processes, procedures, and responsibilities within AT&T, are consistent with the controls documented within the generally accepted international security management standard ISO/IEC 27001:2005.

(b) **Classification of Information** – AT&T uses a multi-tiered information classification framework for categorizing and labeling information based on sensitivity of the content and specific legal requirements.

(c) **Information and Media Handling** – AT&T security standards specify the means and levels of protection for information in transit or in storage with regard to the type of environment and media and within each information classification. The standards also specify the requirements for information destruction and media sanitization.

(d) **Physical Access Controls** – AT&T maintains appropriate physical security practices that include the use of physical monitoring and intrusion detection systems, implementation of locks and access barriers, and screening access to facilities and equipment.

(e) **Logical Access Controls** – AT&T maintains appropriate logical access controls that include authentication of claimed identity (using means such as passwords, PINS or tokens), periodic review of user IDs and accounts to verify continued business need, and management of user privileges in accordance with job function and business need. Password rules follow strict requirements, including a minimum number and type of characters and uniqueness from previous user passwords, user name or dictionary words.

(f) **Network Perimeter Protection** – AT&T employs firewalls that screen incoming and outgoing traffic, and intrusion detection tools that detect unauthorized attempts to penetrate AT&T's global network. AT&T does not monitor individual customer connections for intrusions except when part of a managed security service provided for an additional fee.

(g) **Workstation Security Management** – AT&T uses a variety of processes and technologies that include anti-malware protection and updates, personal firewall, operating system hardening and updates, power-on passwords, password-protected keyboard or screen locks that automatically trigger through inactivity, and full disk encryption where permitted by law to protect sensitive information on portable assets.

(h) **Security Incident Management** – AT&T uses a disciplined global process for the identification of security incidents and threats in a timely manner to minimize the loss or compromise of information belonging to both AT&T and its customers and to facilitate incident resolution. AT&T 24 x 7 global network monitoring and the AT&T threat management platform and program provide real-time situational awareness and data correlation that support active incident investigation and security event case management.

(i) **Monitoring** – AT&T maintains security audit logs that record access attempts and other security events. AT&T security administration limits user control over system security functions to protect against tampering and unauthorized access.

(j) **Security Advisories** – AT&T internally distributes security advisories that originate from industry security organizations and equipment, software and systems suppliers. Each security advisory is categorized, assigned a severity rating, and published by the AT&T global security organization along with the timeframe within which AT&T will endeavor to resolve the vulnerability in accordance with AT&T security standards.

(k) **Compliance** – AT&T conducts regular tests to determine if security controls are maintained and are functioning in accordance with policy. These initiatives include security status checking and vulnerability testing and management.

3. Internal and External Reviews and Audits

3.1. For certain Services, AT&T retains external auditors for periodic reviews of AT&T's security practices against various standards, such as SSAE16/ISAE3402, SysTrust, and Payment Card Industry (PCI) Data Security Standard (DSS). Additional information about external audits and certifications relevant to the Services is available from Customer's AT&T account team upon request. AT&T will provide Service Organization Control (SOC) audit reports to Customer for any audits of the Services against the SSAE16/ISAE3402 standards that AT&T undertakes as part of its general business operations. AT&T shall provide these reports to Customer upon request. Such reports are AT&T's Confidential Information and will be subject to restrictions on use and disclosure.

4. Customer Inquiries and Audits

4.1. Upon request AT&T will enter into discussions in an effort to address Customer's questions concerning the AT&T Security Program. In addition, once during a rolling 12 month period AT&T will also respond to a reasonable number of formal written questions (e.g., a questionnaire) concerning the AT&T Security Program. If AT&T's involvement in responding to such questions and concerns is more than periodic and limited in nature, Customer and AT&T will agree upon the fees to be paid by Customer to AT&T to cover costs that are not reflected in rates and charges for Services.

4.2. If the discussions and responses, along with available reports of independent auditors, do not satisfy Customer's needs, Customer may request to conduct its own security audit of certain AT&T facilities or services. No audit will be conducted until the parties have mutually agreed on the scope, time frame, and location of the audit. If Customer intends to use a third party to conduct an audit or tests, the third party will be required to enter into an appropriate non-disclosure agreement with AT&T prior to commencing the audit or testing. Audits and tests may not be conducted by third parties who are direct competitors of AT&T without AT&T's written consent or by third parties who have previously misused or misappropriated AT&T's confidential information. For some services, AT&T may require a separate written agreement setting forth specific terms and conditions for audits or tests. The following terms and conditions will generally apply to all audits, and there may be other terms or restrictions as well:

(a) AT&T reserves the right to charge Customer reasonable fees that are proportional to AT&T's anticipated costs for providing access to facilities, information and personnel in the course of facilitating the audit.

(b) Audits will be performed according to AT&T Security requirements and will be limited to once per rolling twelve (12) month period during normal AT&T business hours for the identified location.

(c) AT&T will require adequate protection for AT&T's Confidential Information. AT&T will not make any disclosure which would result in the disclosure of information about other AT&T customers or services.

(d) There may be a limit on the number of onsite auditors.

(e) No copies may be taken of any documents (whether electronic or in hard copy) provided during the course of the audit and no document may be removed from the area where documents are available for inspection.

(f) Physical security audits and on-site reviews of AT&T operational facilities and locations will be subject to policies maintained by AT&T Asset Protection and AT&T Corporate Real Estate or their successor organizations.

4.3. If Customer is subject to regulation and audit by governmental or other regulatory authorities having authority to examine Customer's records, AT&T will provide reasonable assistance as requested by Customer to facilitate such examinations, subject to Customer's agreement to pay reasonable fees that are proportional to AT&T's anticipated costs in facilitating the examination, and subject to the restrictions and conditions similar to those described above.

4.4. If Customer identifies a security issue during a discussion, response, audit or test, which Customer reasonably identifies as causing an unacceptable level of threat to Customer, then AT&T will work cooperatively with Customer to determine if another service with a different type or level of security might be more suitable for Customer, or if there are commercially reasonable changes that AT&T might make without altering the cost, functionality or general characteristics of the Service in question.

4.5. AT&T will review Customer's request to perform vulnerability or other testing activities on a service-by-service basis. Such activities will be subject to additional terms and conditions in order to protect AT&T infrastructure and the services and data of other AT&T customers. No tests may be conducted until the parties have entered into a separate written agreement setting forth the scope of the testing and associated terms and conditions.

5. Security Incidents

5.1. If AT&T discovers that a third party has obtained unauthorized access to Customer's data during a security breach of AT&T's network and/or data storage facilities, AT&T will promptly conduct an investigation to determine when, and if possible, how the breach occurred, and will notify the Customer of such breach. AT&T will reasonably assist Customer in investigating and assessing the extent and nature of the breach and will reasonably inform Customer of the progress of AT&T's investigation and its remediation and prevention efforts. Similarly, if Customer becomes aware of any security breach that affects the Services, Customer will promptly notify AT&T of such breach and will reasonably inform AT&T of the progress of and resolution of Customer's investigation. Customer and AT&T will each provide to the other contact information for such notifications and reporting.

6. Customer's General Security Responsibilities

6.1. Customer is responsible for establishing and implementing policies and procedures to safeguard its data and sensitive information against unauthorized access or use. Customer may have additional security responsibilities, depending on the nature of the AT&T Services used by Customer. With respect to use of AT&T Services, these responsibilities include the following, without limitation:

(a) Selecting and implementing appropriate security measures (which may include encryption) based on the nature of the Services Customer uses and the type of information Customer transmits or stores via the Services.

(b) Selecting and using appropriate AT&T Services, security features and options, based on Customer's specific business practices, security requirements and the type of information Customer transmits or stores via the Services.

(c) Developing and maintaining appropriate management and security procedures, such as physical and logical access controls and processes (e.g., application logon security, including unique user identifications and passwords/pins/tokens complying with prudent security policies) on any Customer-provisioned or managed networked devices and systems.

(d) Protecting and providing physical security of devices and systems on Customer's premises, including preventing unauthorized sensors, sniffers and eavesdropping devices from being installed on devices and systems located on Customer's premises.

(e) Ensuring no security testing or scanning is initiated by Customer or its employees, agents or contractors on: (i) AT&T's network; or (ii) application components outside the responsibility and ownership of Customer, except pursuant to the terms of a separate written agreement with AT&T.

(f) Promptly notifying AT&T of any actual or suspected security incidents or vulnerabilities Customer discovers relating to the Services.

7. AT&T Security Products and Services

7.1. AT&T offers managed security products and services designed to assess and protect network infrastructure. Information about managed security products and services is available from Customer's account team. From time to time AT&T may offer some customized services. Execution of the Master Agreement by AT&T is not intended to imply, and will not be interpreted as implying, that any managed security service products or services, or any security-related service options offered by AT&T for a fee, will be provided to Customer free of charge.

Attachment C: Scope of Services Awarded to Contractor

Contractor offers the following service models under this Master Agreement.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Saas	X	X	X	AT&T Conferencing with Cisco WebEx AT&T Video Meetings with Blue Jeans AT&T Cloud Web Security Service AT&T Hosted Contact Center Service
IaaS	X	X	X	AT&T Distributed Denial of Service (DDoS) Defense Service AT&T Unified Communications as a Service AT&T Premises-Based Firewall Service AT&T Managed Intrusion Detection/Intrusion Prevention Service AT&T Professional Services AT&T Content Delivery Network Service
PaaS	X	X	X	

This document provides purchasing entities and eligible users a quick snap shot of the cloud solutions that Contractor provides.

AT&T Conferencing with Cisco WebEx SaaS

Item Name	Description	Units	List MRC	List OTC	Discount MRC %	Discount OTC %	Net MRC	Net OTC
WebEx Meeting Center up to 25 Participants, including the Host								
WebEx Meeting CenterNamed Host-Tier 25-49 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	70%	0%	$ 60.00	$ -
WebEx Meeting Center Named Host-Tier 50-99 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	75%	0%	$ 50.00	$ -
WebEx Meeting Center Named Host-Tier 100 - 199 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	77%	0%	$ 45.00	$ -
WebEx Meeting Center Named Host-Tier 200 - 399 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	81%	0%	$ 37.50	$ -
WebEx Meeting Center Named Host-Tier 400 - 499 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	82%	0%	$ 35.00	$ -
WebEx Meeting Center Named Host-Tier 500 - 749 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	86%	0%	$ 27.50	$ -
WebEx Meeting Center Named Host-Tier 750 - 999 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	87%	0%	$ 25.00	$ -
WebEx Meeting Center Named Host-Tier 1,000 - 1,499 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	89%	0%	$ 22.50	$ -
WebEx Meeting Center Named Host-Tier 1,500 - 2,499 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	90%	0%	$ 20.00	$ -
WebEx Meeting Center Named Host-Tier 2,500 - 4,999 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	92%	0%	$ 15.00	$ -
WebEx Meeting Center Named Host-Tier 5,000 - 7,499 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	93%	0%	$ 13.00	$ -
WebEx Meeting Center Named Host-Tier 7,500 - 9,999 Monthly Named Hosts	Named Host, up to 25 Participants, including the Host	per month, per host account	$ 199.00	$ -	94%	0%	$ 12.00	$ -
WebEx Meeting Center up to 200 Participants, including the Host								

AT&T Conferencing with Cisco WebEx SaaS

Item Name	Description	Units	List MRC	List OTC	Discount MRC %	Discount OTC %	Net MRC	Net OTC
WebEx Meeting CenterNamed Host-Tier 50-74 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	67%	0%	$ 65.00	$ -
WebEx Meeting Center Named Host-Tier 75-99 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	70%	0%	$ 60.00	$ -
WebEx Meeting Center Named Host-Tier 100 - 199 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	74%	0%	$ 52.00	$ -
WebEx Meeting Center Named Host-Tier 200 - 299 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	78%	0%	$ 44.00	$ -
WebEx Meeting Center Named Host-Tier 300 - 399 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	78%	0%	$ 43.00	$ -
WebEx Meeting Center Named Host-Tier 400 - 499 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	80%	0%	$ 40.00	$ -
WebEx Meeting Center Named Host-Tier 500 - 749 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	83%	0%	$ 34.00	$ -
WebEx Meeting Center Named Host-Tier 750 - 999 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	84%	0%	$ 32.00	$ -
WebEx Meeting Center Named Host-Tier 1,000 - 1,499 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	85%	0%	$ 30.00	$ -
WebEx Meeting Center Named Host-Tier 1,500 - 2,499 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	87%	0%	$ 26.00	$ -
WebEx Meeting Center Named Host-Tier 2,500 - 4,999 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	89%	0%	$ 21.00	$ -
WebEx Meeting Center Named Host-Tier 5,000 - 7,499 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	91%	0%	$ 18.00	$ -

AT&T Conferencing with Cisco WebEx SaaS

Item Name	Description	Units	List MRC	List OTC	Discount MRC %	Discount OTC %	Net MRC	Net OTC
WebEx Meeting Center Named Host-Tier 7,500 - 9,999 Monthly Named Hosts	Named Host, up to 200 Participants, including the Host	per month, per host account	$ 199.00	$ -	92%	0%	$ 16.50	$ -
WebEx Meeting Center Committed Minutes with up to 200 Participants, including the Host								
WebEx Meeting Center Committed Minutes-Tier 1,500-4,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	14%	0%	$ 0.25	$ -
WebEx Meeting Center Committed Minutes-Tier 5,000-9,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	17%	0%	$ 0.24	$ -
WebEx Meeting Center Committed Minutes-Tier 10,000-24,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	21%	0%	$ 0.23	$ -
WebEx Meeting Center Committed Minutes-Tier 25,000-49,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	24%	0%	$ 0.22	$ -
WebEx Meeting Center Committed Minutes-Tier 50,000-99,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	31%	0%	$ 0.20	$ -
WebEx Meeting Center Committed Minutes-Tier 100,000-249,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	34%	0%	$ 0.19	$ -
WebEx Meeting Center Committed Minutes-Tier 250,000-499,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	38%	0%	$ 0.18	$ -
WebEx Meeting Center Committed Minutes-Tier 500,000-999,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	45%	0%	$ 0.16	$ -

AT&T Conferencing with Cisco WebEx SaaS

Item Name	Description	Units	List MRC	List OTC	Discount MRC %	Discount OTC %	Net MRC	Net OTC
WebEx Meeting Center Committed Minutes-Tier 1,000,000-2,499,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	48%	0%	$ 0.15	$ -
WebEx Meeting Center Committed Minutes-Tier 5,000,000-9,999,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	52%	0%	$ 0.14	$ -
WebEx Meeting Center Committed Minutes-Tier 2,500,000-4,999,999 Committed Monthly Minutes of Use	Named Host, up to 200 Participants, including the Host	Per minute, per participant	$ 0.29	$ -	55%	0%	$ 0.13	$ -
AT&T Reservationless Audio Toll Free Dial-In (US)								
AT&T Reservationless Audio Toll Free Dial-In (US)	Up to 250 audio participants	Per minute, per participant	$ 0.085	$ -	66%	0%	$ 0.03	$ -

AT&T Video Meetings with Blue Jeans PaaS

Product or Service Orderable Items			List Price	List Price	NASPO Discount		Net Price	Net Price
Component	**Description**	**Units (price per ...)**	**Unit NRC**	**Unit MRC**	**NRC Discount**	**MRC Discount**	**Unit NRC**	**Unit MRC**
Bluejeans Plans								
NAMED HOST PLAN	The Blue Jeans Enterprise Named Host Plan is perfect for organizations looking to scale and customize their Blue Jeans deployments. It enables you to host large meetings with up to 100 participants, record and share meetings, and add your company's branding to Blue Jeans. Dedicated Customer Success Manager (provide user training, adoption and usage support) PSTN Audio Phone Conference Bridge Support Basic support (for Named Hosts and meeting participants) HD screen sharing, video sharing, and chat Interoperability between H.323 or SIP room systems, browsers, MS Lync, Cisco Jabber, and mobile Android or iOS devices	License		$ 149.90	0%	**70%**	$ -	$ 45.00
VIRTUAL PORTS PLAN	Blue Jeans' cloud-based, multi-party video conferencing service provides a cost-effective, scalable alternative to traditional hardware/software-based infrastructure. Our robust video communications platform offers a solution that actually meets the needs of both business users and IT administrators. With easy scheduling, simple click-to-join meetings and Group Administration features, Blue Jeans makes hosting and managing video meetings easy for everyone. Provision unlimited user accounts with all users share the ports on first-come, first-serve basis Dedicated Customer Success Manager (provide user training, adoption and usage support) Basic support (for Named Hosts and meeting participants) HD screen sharing, video sharing, and chat Interoperability between H.323 or SIP room systems, browsers, MS Lync, Cisco Jabber, and mobile Android or iOS devices	Per Port- see below:			0%	0%	$ -	$ -
Virtual Plan 4 to 9 Simultaneous Ports	Virtual Plan 4 to 9 Simultaneous Ports	per port		$ 288.00	0%	0%	$ -	$ 288.00
Virtual Plan 10 to 19 Simultaneous Ports	Virtual Plan 10 to 19 Simultaneous Ports	per port		$ 259.00	0%	0%	$ -	$ 259.00
Virtual Plan 20 or more Simultaneous Ports	Virtual Plan 20 or more Simultaneous Ports	per port		$ 229.00	0%	0%	$ -	$ 229.00
Virtual Plan Port in use Overage charges	Overage charges is per port/per day over committed quantity selected above.	per port	$ 86.00		0%	0%	$ 86.00	$ -
PRIMETIME	Blue Jeans Primetime is a self-service, cloud-based platform that enables presenters to interact over video and stream their event to thousands of viewers. Present, watch or listen from a computer, room system, or mobile device – providing access for everyone, no matter where they are. PSTN is not available at this time.				0%	0%	$ -	$ -
Primetime - 250	Available for up to 250 simultaneous attendees. Priced per event. This can be prepaid or paid on a monthly basis. Includes Enhanced Recording at no added charge.		$ 2,000.00		0%	0%	$ 2,000.00	$ -
Primetime - 500	Available for up to 500 simultaneous attendees. Priced per event. This can be prepaid or paid on a monthly basis. Includes Enhanced Recording at no added charge.		$ 2,500.00		0%	0%	$ 2,500.00	$ -

AT&T Video Meetings with Blue Jeans PaaS

Product or Service Orderable Items			List Price	List Price	NASPO Discount		Net Price	Net Price
Component	**Description**	**Units (price per ...)**	**Unit NRC**	**Unit MRC**	**NRC Discount**	**MRC Discount**	**Unit NRC**	**Unit MRC**
Primetime -1000	Available for up to 1000 simultaneous attendees. Priced per event. This can be prepaid or paid on a monthly basis. Includes Enhanced Recording at no added charge.		$ 3,500.00		0%	0%	$ 3,500.00	$ -
Primetime - 2000	Available for up to 2000 simultaneous attendees. Priced per event. This can be prepaid or paid on a monthly basis. Includes Enhanced Recording at no added charge.		$ 4,500.00		0%	0%	$ 4,500.00	$ -
Attendee Overage	Attendee Overage Charged in 100 Attendees increments		$ 500.00		0%	0%	$ 500.00	$ -
Duration Overage	Duration Overage Charged Per 30 min increments		$ 1,000.00		0%	0%	$ 1,000.00	$ -
Premium Support Package	Increase to Monthly Recurring Charge (MRC) Per Named Host Plan and/or Ports Plan. Calculated against total contract revenue per year. **Package includes:** 24/7/365 phone and internet support provided by BJN One hour response for severity 1 issues Two hour repsonse for severity 2 issues Support during planning and deployment Customer adminstrator training	Additional 25% MRC			0%	0%	$ -	$ -
Meeting Assist 1st Hour	Minimum 1 hour, any time over 1 hour is billed in 30 minute increments. Example: For a meeting that is 1 hour and 40 minutes the charge is: $250 for the first hour, and $125 each for two ($250) 30 minute increments for a total for $500		$ 250.00					
Meeting Assist Added 30 minutes	Minimum 1 hour, any time over 1 hour is billed in 30 minute increments. Example: For a meeting that is 1 hour and 40 minutes the charge is: $250 for the first hour, and $125 each for two ($250) 30 minute increments for a total for $500		$ 125.00					

AT&T Cloud Web Security Service

	Product or Service Orderable Items			List Price	List Price	NASPO Discount		Net Price	Net Price
Subcategory	Component	Description	Units	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
Security	AT&T Cloud Web Security Service	URL Web Filtering	Per Seat	$ -	$ 0.98	0%	15%	$ -	$ 0.83

AT&T Distributed Denial Of Service (DDOS) Defense Services IaaS

Product or Service Orderable Items		List Price	List Price	NASPO Discount		Net Price	Net Price
Component	Units	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
70 Hour Monthly Mitigation Plan	Per Plan	$5,000	$5,000	10%	10%	$ 4,500	$ 4,500
110 Hour Monthly Mitigation Plan	Per Plan	$5,000	$12,143	50%	50%	$ 2,500	$ 6,072
215 Hour Monthly Mitigation Plan	Per Plan	$5,000	$21,428	10%	10%	$ 4,500	$ 19,285
410 Hour Monthly Mitigation Plan	Per Plan	$5,000	$36,428	10%	10%	$ 4,500	$ 32,785
Unlimited Monthly Mitigation Plan	Per Plan	$5,000	$50,000	10%	10%	$ 4,500	$ 45,000
						$ -	$ -
Hourly Overage Charge for 110 hour plan only	Per Hour	$195		100%	0%	$ -	$ -
Hourly Overage Charge	Per Hour	$195		0%	0%	$ 195	$ -
Carrier Agnostic Option**							
Per Customer-Protected Circuit	Lot	$2,500	$1,500	50%	10%	$ 1,250	$ 1,350

***NRC Discount:**

AT&T Distributed Denial Of Service (DDOS) Defense Services IaaS

Product or Service Orderable Items		List Price	List Price	NASPO Discount		Net Price	Net Price
Component	Units	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
**Customers must choose a Monthly Mitigation Plan. Per Customer-Protected Circuit Charges appear on a separate line item in addition to the chosen Plan ***Additional Details: 1. Only Local and State Government and Education customers qualify for this offer. 2. 60% discount only applies if the client chooses the 110 hour rate plan. For the 70 hour rate plan or any other rate plan, standard field authority applies within this exclusive offer. 3. 100% discount on the Overage component only applies if the client chooses the 110 hour rate plan. When the 70 hour or any other rate plan is chosen, no discount is available on the Overage component. 4. DDoS Defense is not an E-rate eligible service							

Unified Communications Pricing / Discounting Rates:

LEAD VOICE AND BUNDLED VOICE OFFERS:

AT&T Unified Communications Pricing

Product Description	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC	Comments
Base Packages								
Essential	Per Named User	$11.99	$ -	47%		$ 6.35	$ -	250 User Minimum. If over 999 users obtain custom pricing
Essential Plus	Per Named User	$ 16.99	$ -	52%		$ 8.16	$ -	250 User Minimum. If over 999 users obtain custom pricing
Classic	Per Named User	$ 23.99	$ -	58%		$ 10.08	$ -	250 User Minimum. If over 999 users obtain custom pricing
Enhanced	Per Named User	$ 25.99	$ -	47%		$ 13.77	$ -	250 User Minimum. If over 999 users obtain custom pricing
Installation and MACD								
New Site Installation Fee	Per Site, Per Hour	$ -	$ 195.00		0%	$ -	$ 195.00	Per Site, Per Hour charge for new site installation
Project MACD Fee	Per Hour	$ -	$ 195.00		0%	$ -	$ 195.00	Per Hour fee for Moves, Adds, Changes, Deletes
Optional Features								
Unified Messaging	Per Named User	$ 10.99	$ -	32%		$ 7.47	$ -	250 User Minimum. If over 999 users obtain custom pricing
Voice Mail	Per Named User	$ 8.49	$ -	32%		$ 5.77	$ -	250 User Minimum. If over 999 users obtain custom pricing
Federation	Per Named User	$ 4.99	$ -	47%		$ 2.64	$ -	250 User Minimum. If over 999 users obtain custom pricing
Auto Attendant - 1-4 Options	Per Named User	$ 8.49	$ -	32%		$ 5.77	$ -	250 User Minimum. If over 999 users obtain custom pricing
Auto Attendant - 5+ Options	Per Named User	$ 10.99	$ -	32%		$ 7.47	$ -	250 User Minimum. If over 999 users obtain custom pricing
Advanced E911	Per Named User	$ 1.50	$ -	0%		$ 1.50	$ -	250 User Minimum. If over 999 users obtain custom pricing
PBX Integration Point (PIP)	Concurrent Calls -1- 50	$ 4.99	$ -	0%		$ 4.99	$ -	Up to 50 Concurrent calls
PBX Integration Point (PIP)	Concurrent Calls- 51+	$ 3.99	$ -	0%		$ 3.99	$ -	51 Concurrent calls and more
UC Attendant Console	Per Operator 1-3	$ 220.00	$ -	4%		$ 211.20	$ -	Price is per Operator. Maximum 3
UC Attendant Console	Per Operator 4-6	$ 230.00	$ -	4%		$ 220.80	$ -	Price is per Operator. Maximum 6
UC Attendant Console	Per Operator 7-10	$ 245.00	$ -	4%		$ 235.20	$ -	Price is per Operator. Maximum 10
Attendant Console - Standard (Serverless)	Per User	$ 36.50	$ -	0%		$ 36.50	$ -	Price is per Attendant Console-Standard (Serverless)
Group Announcements Basic & Advanced	Endpoints 1-50	$ 200.00	$ -	0%		$ 200.00	$ -	Price is for up to 50 endpoints.
Group Announcements Basic & Advanced	Endpoints 51+	$ 325.00	$ -	0%		$ 325.00	$ -	Price is for up to 51 endpoints and more.
Collaboration Edge	20- 50 Users	$ 35.00	$ -	0%		$ 35.00	$ -	Price is per User
Collaboration Edge	51- 99 Users	$ 15.00	$ -	0%		$ 15.00	$ -	Price is per User
Collaboration Edge	100- 499 Users	$ 7.50	$ -	0%		$ 7.50	$ -	Price is per User
Esna Cloudlink for Cisco®	Per User	$ 2.25	$ -	0%		$ 2.25	$ -	Price is per User
Esna iLink integration	Per User	$ 1.50	$ -	0%		$ 1.50	$ -	Price is per User
Cisco Collaboration Meeting Room (CMR Cloud)	Per Company	$ 70.00	$ -	0%		$ 70.00	$ -	Charge of $4.99 (1-50)/$3.99 (51+) per Concurrent Call Path
Cisco TelePresence Conductor Configuration	Per Company MRC**	$ 600.00	$ -	0%		$ 600.00	$ -	Customers purchasing Telepresence will also pay a Non-Recurring
UC Services Connection	Bandwidth up to:							Price is based on bandwidth selected.
UC Services Connection	10 MB	$ 360.00	$ -	54%		$ 165.60	$ -	
UC Services Connection	20 MB	$ 710.00	$ -	54%		$ 326.60	$ -	
UC Services Connection	30 MB	$ 1,055.00	$ -	54%		$ 485.30	$ -	
UC Services Connection	40 MB	$ 1,385.00	$ -	54%		$ 637.10	$ -	
UC Services Connection	50 MB	$ 1,710.00	$ -	54%		$ 786.60	$ -	
UC Services Connection	60 MB	$ 2,025.00	$ -	54%		$ 931.50	$ -	
UC Services Connection	70 MB	$ 2,330.00	$ -	54%		$ 1,071.80	$ -	
UC Services Connection	80 MB	$ 2,630.00	$ -	54%		$ 1,209.80	$ -	
UC Services Connection	90 MB	$ 2,915.00	$ -	54%		$ 1,340.90	$ -	
UC Services Connection	100 MB	$ 3,195.00	$ -	54%		$ 1,469.70	$ -	
UC Services Connection	150 MB	$ 4,725.00	$ -	54%		$ 2,173.50	$ -	
UC Services Connection	200 MB	$ 6,210.00	$ -	54%		$ 2,856.60	$ -	
UC Services Connection	250 MB	$ 7,650.00	$ -	54%		$ 3,519.00	$ -	

Unified Communications Pricing / Discounting Rates:

LEAD VOICE AND BUNDLED VOICE OFFERS:

AT&T Unified Communications Pricing								
UC Services Connection	300 MB	$ 9,045.00	$ -	54%		$ 4,160.70	$ -	
UC Services Connection	400 MB	$ 11,880.00	$ -	54%		$ 5,464.80	$ -	
UC Services Connection	450 MB	$ 13,160.00	$ -	54%		$ 6,053.60	$ -	
UC Services Connection	500 MB	$ 14,625.00	$ -	54%		$ 6,727.50	$ -	
UC Services Connection	600 MB	$ 17,280.00	$ -	54%		$ 7,948.80	$ -	
UC Services Connection	700 MB	$ 19,845.00	$ -	54%		$ 9,128.70	$ -	
UC Services Connection	800 MB	$ 22,320.00	$ -	54%		$ 10,267.20	$ -	
UC Services Connection	900 MB	$ 24,705.00	$ -	54%		$ 11,364.30	$ -	
UC Services Connection	1000 MB	$ 27,000.00	$ -	54%		$ 12,420.00	$ -	

AT&T Hosted Contact Center Service PaaS

Core Platform Components										
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
Base Configured User License	The number of unique configured users for the selected time period. • Agent • ACD Voice Queuing & Routing • Call Monitoring • Callback queuing • 1 Universal Port	858	User		150	10%	10%	$ -	$ 135
Base Configured Station License	A **station** is a physical location or phone where an agent will work and communicate with contacts, whether it's a home office, call center workstation, etc. When the station is created, the system auto-generates a unique Station ID. A based configured station is the number of configured, active stations plus the number of agent-created stations (created by entering a phone number). • ACD Voice Queuing & Routing • Call Monitoring • Callback queuing	859	Comfigured User		195			$ -	$ 195

AT&T Hosted Contact Center Service PaaS

Core Platform Components									
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
	• 1 Universal Port								
Base Concurrent User License	The number of agents who logged in the system simultaneously for the selected time period. • ACD Voice Queuing & Routing • Call Monitoring • Callback queuing • 1 Universal Port	3260	Concurrent User		210			$ -	$ 210
PCI Level 1 per Configured User License	• Agent • ACD Voice Queuing & Routing • Call Monitoring • Call Back Queuing • 1 Universal Port This offering is required to include accompanying parts 3148 ["Universal Port (Configured user)"] and 3152 ["Storage (Configured user)"]	PCI858							
PCI Level 1 per Concurrent Agent	• Agent • ACD Voice Queuing & Routing • Call Monitoring • Call Back Queuing • 1 Universal Port This offering is required to include accompanying parts 3151 ["Universal Port (Concurrent user)"] and 3154 ["Storage (Concurrent user)"]	PCI3260	Concurrent Agent		234			$ -	$ 234
	• A port is a measure of the maximum number of simultaneous phone calls permitted for an inContact business unit.								

AT&T Hosted Contact Center Service PaaS

Core Platform Components										
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
Disaster Recovery Port Reservation	• One port supports the ability to handle one voice-related (phone) contact • A port can be used for inbound calls (for IVR, ACD, or "pass-through" transfers) or outbound calls (agent-requested dials, dialer / callback / or other system generated dials, or the outbound leg of call transfers) • One port is included with each user license. Additional "stand-alone" ports may be required to properly support activities such as ACD queuing, IVR-only implementations (where no stations have been purchased), or campaign dialing programs (such as predictive dialing) where more the number of simultaneous calls often exceeds the number of stations. • These ports are required when base licenses are purchased. The ordered quantity is factored into the number of total ports originally configured, but the actual monthly invoice is based on usage (which is the difference between the total number of ports on the business unit and the number of ports included with the base and • If no additional ports are needed (beyond what is included with the core and Personal Connection licenses), the quote / order should simply indicate a quantity of zero (0).	1603	Port		75			$ -	$ 75
Chat & Email ***User Add-on***	ACD Chat Queuing & Routing ACD Email Queuing & Routing	877	User		10			$ -	$ 10
Voice Recording *with Storage* ***User Add-on***	Unlimited agent call recording One (1) Gigabyte of storage is included with each Voice Recording with Storage add-on	799	GigaByte		10			$ -	$ 10

AT&T Hosted Contact Center Service PaaS

Core Platform Components									
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
Universal Port	• A port is a measure of the maximum number of simultaneous phone calls permitted for an inContact (customer) business unit. • One port supports the ability to handle one voice-related (phone) contact • One port is included with each user license. • Additional "stand-alone" ports may be required to properly support activities such as ACD queuing, IVR-only implementations (where no stations have been purchased), or campaign dialing programs (such as predictive dialing) where the number of simultaneous calls often exceeds the number of stations. • Measured per peak number of total ports configured during the billing interval LESS the peak number of user licenses for the billing interval. (One port is included with the purchase of each user license.) • A port provides access for inbound calls (for IVR, ACD, or "pass-through" transfers) or outbound calls (agent-requested dials, dialer / callback / or other system generated dials, or the outbound leg of call transfers). • Additional voice port available for queuing, transfers, IVR, and automated outbound dialing	3148	Configured User		75			$ -	$ 75
		3149	Configured Station		75			$ -	$ 75

AT&T Hosted Contact Center Service PaaS

Core Platform Components									
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
	• Text-to-Speech IVR playback	3151	Concurrent User		75			$ -	$ 75
Storage	1 Gb disk storage *Note: For each business unit, the first Gb is free. Storage is usage-based, meaning inContact charges per on actual utilization and may vary from month to month. Storage is determined by the peak number of gigabytes of disk space used during a month LESS any storage included with the Voice Recording add-on, if applicable.*	3152	Configured User		10			$ -	$ 10
		3153	Configured Station		10			$ -	$ 10
		3154	Concurrent User		10			$ -	$ 10
Personal Connection Dialer Configured User License ***User Add-on***	Outbound solution that eliminates awkward delays when greeting a caller as agents make multiple predictive calls. Agents are connected at the first hello, which enables better outcomes, higher conversion rates, and increased revenues. • Customers never silently wait for an agent to answer • Higher agent productivity with predictive dialing • Maintain compliance with government regulations • Customize calling campaigns • Intelligent Call Suppression • Proactive XS synchronizes external systems	3613	Configured Station		30			$ -	$ 30

AT&T Hosted Contact Center Service PaaS

Core Platform Components									
Standard Options Product	Description / Inclusion(s)	CatID	Units (price per ...)	List Price Unit NRC	List Price Unit MRC	NASPO Discount NRC Discount	NASPO Discount MRC Discount	Net Price Unit NRC	Net Price Unit MRC
	Note that this add-on can be applied to Configured User, Configured Station, and Concurrent Agent base billing licenses, but this add-on is based on the number of Configured Users irrespective of the base billing model.								
Personal Connection Dialer Concurrent User License ***User Add-on***	Outbound solution that eliminates awkward delays when greeting a caller as agents make multiple predictive calls. Agents are connected at the first hello, which enables better outcomes, higher conversion rates, and increased revenues. • Customers never silently wait for an agent to answer • Higher agent productivity with predictive dialing • Maintain compliance with government regulations • Customize calling campaigns • Intelligent Call Suppression • Proactive XS synchronizes external systems	3471	Concurrent User		42			$ -	$ 42

AT&T Hosted Contact Center Service PaaS

Core Platform Components										
Standard Options Product	Description / Inclusion(s)	CatID		List Price	List Price	NASPO Discount		Net Price	Net Price
			Units (price per ...)	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
	Note that this add-on can be applied to Concurrent Agent base billing licenses, but this add-on is based on the number of Configured Users irrespective of the base billing model.								
Agent Scripting ***User Add-on***	Design and deploy custom browser forms for agent use with inbound and outbound calls	876	core license		30			$ -	$ 30
inContact Agent for Salesforce	Native Salesforce.com application for use by contact center agents	3347	Per named User		15			$ -	$ 15
inView	• Dashboard Performance Management • Visibility at Executive, Supervisor and Agent level • Real-time data reporting	3465	Configured User		25			$ -	$ 25
Direct Data Access	Direct Access provides a client with a secure connection from Microsoft Excel directly to the inContact data model for reporting and analytics using their existing inContact user credentials. Offering requires a one-time activation fee and then a monthly-recurring charge for continued access. End-user is required to provide his/her own license to MS Excel 2010 or greater. inContact will provide instructions and support for establishing the Direct Data Access connection from MS Excel, but does NOT provide expertise, services, or resources for Microsoft's Excel product.	3596	Business Unit		1000			$ -	$ 1,000
	Auto Attendant provides Corporate Directory and Voicemail Management features which tightly integrate with the inContact platform. • Seamless integration with the inContact ACD								

AT&T Hosted Contact Center Service PaaS

Core Platform Components									
Standard Options Product	Description / Inclusion(s)	CatID	Units (price per ...)	List Price Unit NRC	List Price Unit MRC	NASPO Discount NRC Discount	NASPO Discount MRC Discount	Net Price Unit NRC	Net Price Unit MRC
Auto Attendant Dial by Ext/Name & VM (per User)	• Transfer inbound callers without live intervention • Centralized voicemail • Dial-by-name, Dial-by-extension, DNIS or company directory • Provides a unified experience to all callers • Connects to mixed telephony and connectivity models • Manageable outside of the Central platform	4029	User		16			$ -	$ 16
Auto Attendant Dial by Ext/Name Only	Auto Attendant provides Corporate Directory features which tightly integrate with the inContact platform. • Seamless integration with the inContact ACD • Transfer inbound callers without live intervention • Dial-by-name, Dial-by-extension, DNIS or company directory • Provides a unified experience to all callers • Connects to mixed telephony and connectivity models • Manageable outside of the Central platform	4030	User		6			$ -	$ 6
Integration: UI, Data, Web	Fee is per interface. • Integration to external data sources are subject to a monthly recurring charge to maintain that ongoing integration • Integration to external data sources typically require a separate one-time implementation service charge	3159							

AT&T Hosted Contact Center Service PaaS

Core Platform Components								
Standard Options Product	Description / Inclusion(s)	CatID	Units (price per ...)	List Price Unit NRC	List Price Unit MRC	NASPO Discount NRC Discount	NASPO Discount MRC Discount	Net Price Unit NRC	Net Price Unit MRC
Services	• The most common data integration utilizes web services supplied by the customer • inContact Professional Services may support other data integration methodologies, subject to inContact approval • Each unique, approved integration data source is considered an "interface"		Per interface		500			$ -	$ 500

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.CheckPoint.2205.SA	Per device	$ 900.00	$ 4,950.00	0%	0%	$ 900.00	$ 4,950.00
PB.FW.CheckPoint.4407.SA	Per device	$ 1,680.00	$ 5,830.00	0%	0%	$ 1,680.00	$ 5,830.00
PB.FW.CheckPoint.4607.SA	Per device	$ 2,200.00	$ 6,350.00	0%	0%	$ 2,200.00	$ 6,350.00
PB.FW.CheckPoint.4807.SA	Per device	$ 3,000.00	$ 6,630.00	0%	0%	$ 3,000.00	$ 6,630.00
PB.FW.CheckPoint.2205.HA	Per device	$ 1,650.00	$ 9,030.00	0%	0%	$ 1,650.00	$ 9,030.00
PB.FW.CheckPoint.4407.HA	Per device	$ 2,680.00	$ 9,030.00	0%	0%	$ 2,680.00	$ 9,030.00
PB.FW.CheckPoint.4607.HA	Per device	$ 3,500.00	$ 9,030.00	0%	0%	$ 3,500.00	$ 9,030.00
PB.FW.CheckPoint.4807.HA	Per device	$ 4,800.00	$ 9,030.00	0%	0%	$ 4,800.00	$ 9,030.00
PB.FW.Cisco.ASA.5515X.SA	Per device	$ 730.00	$ 4,950.00	0%	0%	$ 730.00	$ 4,950.00
PB.FW.Cisco.ASA.5525X.SA	Per device	$ 1,300.00	$ 5,830.00	0%	0%	$ 1,300.00	$ 5,830.00
PB.FW.Cisco.ASA.5545X.SA	Per device	$ 1,900.00	$ 6,350.00	0%	0%	$ 1,900.00	$ 6,350.00
PB.FW.Cisco.ASA.5555X.SA	Per device	$ 2,430.00	$ 6,630.00	0%	0%	$ 2,430.00	$ 6,630.00
PB.FW.Cisco.ASA.5585-S10.SA	Per device	$ 3,080.00	$ 7,380.00	0%	0%	$ 3,080.00	$ 7,380.00
PB.FW.Cisco.ASA.5585-S20.SA	Per device	$ 4,450.00	$ 7,380.00	0%	0%	$ 4,450.00	$ 7,380.00
PB.FW.Cisco.ASA.5585-S40.SA	Per device	$ 7,730.00	$ 7,380.00	0%	0%	$ 7,730.00	$ 7,380.00
PB.FW.Cisco.ASA.5585-S60.SA	Per device	$ 11,530.00	$ 7,380.00	0%	0%	$ 11,530.00	$ 7,380.00
PB.FW.Cisco.ASA.5515X.HA	Per device	$ 1,450.00	$ 9,030.00	0%	0%	$ 1,450.00	$ 9,030.00
PB.FW.Cisco.ASA.5525X.HA	Per device	$ 2,230.00	$ 9,030.00	0%	0%	$ 2,230.00	$ 9,030.00
PB.FW.Cisco.ASA.5545X.HA	Per device	$ 3,300.00	$ 9,030.00	0%	0%	$ 3,300.00	$ 9,030.00
PB.FW.Cisco.ASA.5555X.HA	Per device	$ 4,180.00	$ 9,030.00	0%	0%	$ 4,180.00	$ 9,030.00
PB.FW.Cisco.ASA.5585-S10.HA	Per device	$ 5,380.00	$ 9,030.00	0%	0%	$ 5,380.00	$ 9,030.00
PB.FW.Cisco.ASA.5585-S20.HA	Per device	$ 8,130.00	$ 9,030.00	0%	0%	$ 8,130.00	$ 9,030.00
PB.FW.Cisco.ASA.5585-S40.HA	Per device	$ 14,700.00	$ 9,030.00	0%	0%	$ 14,700.00	$ 9,030.00
PB.FW.Cisco.ASA.5585-S60.HA	Per device	$ 22,300.00	$ 9,030.00	0%	0%	$ 22,300.00	$ 9,030.00
IPT Integrated ASA devices	Per device			0%	0%	$ -	$ -
PB.FW.Cisco.ASA.5515X.SA.IPT	Per device	$ 730.00	$ 4,950.00	0%	0%	$ 730.00	$ 4,950.00
PB.FW.Cisco.ASA.5525X.SA.IPT	Per device	$ 1,300.00	$ 5,830.00	0%	0%	$ 1,300.00	$ 5,830.00
PB.FW.Cisco.ASA.5545X.SA.IPT	Per device	$ 1,900.00	$ 6,350.00	0%	0%	$ 1,900.00	$ 6,350.00
PB.FW.Cisco.ASA.5555X.SA.IPT	Per device	$ 2,430.00	$ 6,630.00	0%	0%	$ 2,430.00	$ 6,630.00
PB.FW.Juniper.SRX220.SA	Per device	$ 500.00	$ 4,950.00	0%	0%	$ 500.00	$ 4,950.00

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Juniper.SRX240.SA	Per device	$ 1,050.00	$ 5,830.00	0%	0%	$ 1,050.00	$ 5,830.00
PB.FW.Juniper.SRX650.SA	Per device	$ 2,050.00	$ 6,350.00	0%	0%	$ 2,050.00	$ 6,350.00
PB.FW.Juniper.SRX1400.SA	Per device	$ 2,800.00	$ 6,630.00	0%	0%	$ 2,800.00	$ 6,630.00
PB.FW.Juniper.SRX220.HA	Per device	$ 1,100.00	$ 9,030.00	0%	0%	$ 1,100.00	$ 9,030.00
PB.FW.Juniper.SRX240.HA	Per device	$ 1,750.00	$ 9,030.00	0%	0%	$ 1,750.00	$ 9,030.00
PB.FW.Juniper.SRX650.HA	Per device	$ 3,550.00	$ 9,030.00	0%	0%	$ 3,550.00	$ 9,030.00
PB.FW.Juniper.SRX1400.HA	Per device	$ 5,050.00	$ 9,030.00	0%	0%	$ 5,050.00	$ 9,030.00
PB.FW.Fortinet.FWF-80CM.SA	Per device	$ 450.00	$ 4,950.00	0%	0%	$ 450.00	$ 4,950.00
PB.FW.Fortinet.100D.SA	Per device	$ 500.00	$ 4,950.00	0%	0%	$ 500.00	$ 4,950.00
PB.FW.Fortinet.300C.SA	Per device	$ 1,150.00	$ 5,830.00	0%	0%	$ 1,150.00	$ 5,830.00
PB.FW.Fortinet.600C.SA	Per device	$ 1,550.00	$ 6,350.00	0%	0%	$ 1,550.00	$ 6,350.00
PB.FW.Fortinet.800C.SA	Per device	$ 1,680.00	$ 6,350.00	0%	0%	$ 1,680.00	$ 6,350.00
PB.FW.Fortinet.1240B.SA	Per device	$ 2,630.00	$ 6,630.00	0%	0%	$ 2,630.00	$ 6,630.00
PB.FW.Fortinet.FWF-80CM.HA	Per device	$ 950.00	$ 9,030.00	0%	0%	$ 950.00	$ 9,030.00
PB.FW.Fortinet.100D.HA	Per device	$ 1,080.00	$ 9,030.00	0%	0%	$ 1,080.00	$ 9,030.00
PB.FW.Fortinet.300C.HA	Per device	$ 1,950.00	$ 9,030.00	0%	0%	$ 1,950.00	$ 9,030.00
PB.FW.Fortinet.600C.HA	Per device	$ 2,500.00	$ 9,030.00	0%	0%	$ 2,500.00	$ 9,030.00
PB.FW.Fortinet.800C.HA	Per device	$ 2,750.00	$ 9,030.00	0%	0%	$ 2,750.00	$ 9,030.00
PB.FW.Fortinet.1240B.HA	Per device	$ 4,600.00	$ 9,030.00	0%	0%	$ 4,600.00	$ 9,030.00
PB.FW.PaloAlto.PA200.SA	Per device	$ 480.00	$ 3,600.00	0%	0%	$ 480.00	$ 3,600.00
PB.FW.PaloAlto.PA500.SA	Per device	$ 1,020.00	$ 4,240.00	0%	0%	$ 1,020.00	$ 4,240.00
PB.FW.PaloAlto.PA3020.SA	Per device	$ 1,950.00	$ 4,620.00	0%	0%	$ 1,950.00	$ 4,620.00
PB.FW.PaloAlto.PA3050.SA	Per device	$ 2,910.00	$ 4,820.00	0%	0%	$ 2,910.00	$ 4,820.00
PB.FW.PaloAlto.PA5020.SA	Per device	$ 3,880.00	$ 5,370.00	0%	0%	$ 3,880.00	$ 5,370.00
PB.FW.PaloAlto.PA5050.SA	Per device	$ 6,770.00	$ 5,370.00	0%	0%	$ 6,770.00	$ 5,370.00
PB.FW.PaloAlto.PA5060.SA	Per device	$ 12,130.00	$ 5,370.00	0%	0%	$ 12,130.00	$ 5,370.00
PB.FW.PaloAlto.PA200.HA	Per device	$ 1,000.00	$ 6,570.00	0%	0%	$ 1,000.00	$ 6,570.00
PB.FW.PaloAlto.PA500.HA	Per device	$ 1,790.00	$ 6,570.00	0%	0%	$ 1,790.00	$ 6,570.00
PB.FW.PaloAlto.PA3020.HA	Per device	$ 3,530.00	$ 6,570.00	0%	0%	$ 3,530.00	$ 6,570.00
PB.FW.PaloAlto.PA3050.HA	Per device	$ 5,260.00	$ 6,570.00	0%	0%	$ 5,260.00	$ 6,570.00

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.PaloAlto.PA5020.HA	Per device	$ 7,860.00	$ 6,570.00	0%	0%	$ 7,860.00	$ 6,570.00
PB.FW.PaloAlto.PA5050.HA	Per device	$ 13,100.00	$ 6,570.00	0%	0%	$ 13,100.00	$ 6,570.00
PB.FW.PaloAlto.PA5060.HA	Per device	$ 23,700.00	$ 6,570.00	0%	0%	$ 23,700.00	$ 6,570.00

STANDARD PBFW OPTIONS - AVAILABLE ON SELECT PLATFORMS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.OPT.ASI	Per device	$ 320.00	$ 2,000.00	0%	0%	$ 320.00	$ 2,000.00
PB.FW.OPT.S2S	Per device	$ 100.00	$ 540.00	0%	0%	$ 100.00	$ 540.00
PB.FW.OPT.C2S	Per device	$ 40.00	$ 670.00	0%	0%	$ 40.00	$ 670.00
PB.FW.OPT.CXE	Per device	$ 240.00	$ 2,000.00	0%	0%	$ 240.00	$ 2,000.00

AT&T Managed Security Services - Premises-Based Firewall Unified Threat Management (UTM) Offers

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Fortinet.FWF-80CM.SA.UTM.Base	Per device	$ 500.00	$ 4,950.00	0%	0%	$ 500.00	$ 4,950.00
PB.FW.Fortinet.100D.SA.UTM.Base	Per device	$ 600.00	$ 4,950.00	0%	0%	$ 600.00	$ 4,950.00
PB.FW.Fortinet.300C.SA.UTM.Base	Per device	$ 1,380.00	$ 5,830.00	0%	0%	$ 1,380.00	$ 5,830.00
PB.FW.Fortinet.600C.SA.UTM.Base	Per device	$ 1,930.00	$ 6,350.00	0%	0%	$ 1,930.00	$ 6,350.00
PB.FW.Fortinet.800C.SA.UTM.Base	Per device	$ 2,130.00	$ 6,350.00	0%	0%	$ 2,130.00	$ 6,350.00
PB.FW.Fortinet.1240B.SA.UTM.Base	Per device	$ 3,550.00	$ 6,350.00	0%	0%	$ 3,550.00	$ 6,350.00
PB.FW.Fortinet.FWF-80CM.HA.UTM.Base	Per device	$ 1,050.00	$ 9,030.00	0%	0%	$ 1,050.00	$ 9,030.00
PB.FW.Fortinet.100D.HA.UTM.Base	Per device	$ 1,250.00	$ 9,030.00	0%	0%	$ 1,250.00	$ 9,030.00

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Fortinet.300C.HA.UTM.Base	Per device	$ 2,400.00	$ 9,030.00	0%	0%	$ 2,400.00	$ 9,030.00
PB.FW.Fortinet.600C.HA.UTM.Base	Per device	$ 3,250.00	$ 9,030.00	0%	0%	$ 3,250.00	$ 9,030.00
PB.FW.Fortinet.800C.HA.UTM.Base	Per device	$ 3,680.00	$ 9,030.00	0%	0%	$ 3,680.00	$ 9,030.00
PB.FW.Fortinet.1240B.HA.UTM.Base	Per device	$ 6,450.00	$ 9,030.00	0%	0%	$ 6,450.00	$ 9,030.00
PB.FW.Juniper.SRX220.SA.UTM.Base	Per device	$ 730.00	$ 6,000.00	0%	0%	$ 730.00	$ 6,000.00
PB.FW.Juniper.SRX240.SA.UTM.Base	Per device	$ 1,330.00	$ 6,000.00	0%	0%	$ 1,330.00	$ 6,000.00
PB.FW.Juniper.SRX650.SA.UTM.Base	Per device	$ 3,200.00	$ 6,000.00	0%	0%	$ 3,200.00	$ 6,000.00
PB.FW.Juniper.SRX1400.SA.UTM.Base	Per device	$ 3,550.00	$ 6,000.00	0%	0%	$ 3,550.00	$ 6,000.00
PB.FW.Juniper.SRX220.HA.UTM.Base	Per device	$ 1,380.00	$ 8,800.00	0%	0%	$ 1,380.00	$ 8,800.00
PB.FW.Juniper.SRX240.HA.UTM.Base	Per device	$ 2,280.00	$ 8,800.00	0%	0%	$ 2,280.00	$ 8,800.00
PB.FW.Juniper.SRX650.HA.UTM.Base	Per device	$ 5,880.00	$ 8,800.00	0%	0%	$ 5,880.00	$ 8,800.00
PB.FW.Juniper.SRX1400.HA.UTM.Base	Per device	$ 6,600.00	$ 8,800.00	0%	0%	$ 6,600.00	$ 8,800.00

STANDARD PBFW-UTM OPTIONS - AVAILABLE ON SELECT PLATFORMS

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.OPT.ASI	Per device	$ 320.00	$ 2,000.00	0%	0%	$ 320.00	$ 2,000.00
PB.FW.OPT.S2S	Per device	$ 100.00	$ 540.00	0%	0%	$ 100.00	$ 540.00
PB.FW.OPT.C2S	Per device	$ 40.00	$ 670.00	0%	0%	$ 40.00	$ 670.00
PB.FW.OPT.CXE	Per device	$ 240.00	$ 2,000.00	0%	0%	$ 240.00	$ 2,000.00
PB.FW.UTM.URL	Per device	$ 160.00	$ 340.00	0%	0%	$ 160.00	$ 340.00
PB.FW.UTM.AV	Per device	$ 160.00	$ 340.00	0%	0%	$ 160.00	$ 340.00
PB.FW.UTM.IDPS	Per device	$ 680.00	$ 940.00	0%	0%	$ 680.00	$ 940.00

AT&T Managed Security Services - Premises-Based Firewall Next Generation (NG) Offers

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
Product Code	**Units**	**MRC**	**OTC**	**MRC Discount**	**OTC Discount**	**Net MRC**	**Net OTC**
PB.FW.PaloAlto.PA200.SA.NG.Bundle	Per device	$ 1,290.00	$ 6,780.00	0%	0%	$ 1,290.00	$ 6,780.00
PB.FW.PaloAlto.PA500.SA.NG.Bundle	Per device	$ 1,860.00	$ 7,620.00	0%	0%	$ 1,860.00	$ 7,620.00
PB.FW.PaloAlto.PA3020.SA.NG.Bundle	Per device	$ 4,150.00	$ 8,100.00	0%	0%	$ 4,150.00	$ 8,100.00
PB.FW.PaloAlto.PA3050.SA.NG.Bundle	Per device	$ 6,240.00	$ 8,350.00	0%	0%	$ 6,240.00	$ 8,350.00
PB.FW.PaloAlto.PA5020.SA.NG.Bundle	Per device	$ 9,620.00	$ 9,090.00	0%	0%	$ 9,620.00	$ 9,090.00
PB.FW.PaloAlto.PA5050.SA.NG.Bundle	Per device	$ 15,910.00	$ 9,090.00	0%	0%	$ 15,910.00	$ 9,090.00
PB.FW.PaloAlto.PA5060.SA.NG.Bundle	Per device	$ 28,500.00	$ 9,090.00	0%	0%	$ 28,500.00	$ 9,090.00
PB.FW.PaloAlto.PA200.HA.NG.Bundle	Per device	$ 1,950.00	$ 10,300.00	0%	0%	$ 1,950.00	$ 10,300.00
PB.FW.PaloAlto.PA500.HA.NG.Bundle	Per device	$ 2,720.00	$ 10,300.00	0%	0%	$ 2,720.00	$ 10,300.00
PB.FW.PaloAlto.PA3020.HA.NG.Bundle	Per device	$ 5,950.00	$ 10,300.00	0%	0%	$ 5,950.00	$ 10,300.00
PB.FW.PaloAlto.PA3050.HA.NG.Bundle	Per device	$ 9,030.00	$ 10,300.00	0%	0%	$ 9,030.00	$ 10,300.00
PB.FW.PaloAlto.PA5020.HA.NG.Bundle	Per device	$ 13,890.00	$ 10,300.00	0%	0%	$ 13,890.00	$ 10,300.00
PB.FW.PaloAlto.PA5050.HA.NG.Bundle	Per device	$ 23,270.00	$ 10,300.00	0%	0%	$ 23,270.00	$ 10,300.00
PB.FW.PaloAlto.PA5060.HA.NG.Bundle	Per device	$ 42,000.00	$ 10,300.00	0%	0%	$ 42,000.00	$ 10,300.00
PB.FW.PaloAlto.PA200.SA.NG.Base	Per device	$ 790.00	$ 3,600.00	0%	0%	$ 790.00	$ 3,600.00
PB.FW.PaloAlto.PA500.SA.NG.Base	Per device	$ 1,550.00	$ 4,240.00	0%	0%	$ 1,550.00	$ 4,240.00
PB.FW.PaloAlto.PA3020.SA.NG.Base	Per device	$ 3,620.00	$ 4,620.00	0%	0%	$ 3,620.00	$ 4,620.00
PB.FW.PaloAlto.PA3050.SA.NG.Base	Per device	$ 5,800.00	$ 4,820.00	0%	0%	$ 5,800.00	$ 4,820.00
PB.FW.PaloAlto.PA5020.SA.NG.Base	Per device	$ 8,930.00	$ 5,370.00	0%	0%	$ 8,930.00	$ 5,370.00
PB.FW.PaloAlto.PA5050.SA.NG.Base	Per device	$ 15,170.00	$ 5,370.00	0%	0%	$ 15,170.00	$ 5,370.00
PB.FW.PaloAlto.PA5060.SA.NG.Base	Per device	$ 27,640.00	$ 5,370.00	0%	0%	$ 27,640.00	$ 5,370.00
PB.FW.PaloAlto.PA200.HA.NG.Base	Per device	$ 1,330.00	$ 6,570.00	0%	0%	$ 1,330.00	$ 6,570.00
PB.FW.PaloAlto.PA500.HA.NG.Base	Per device	$ 2,390.00	$ 6,570.00	0%	0%	$ 2,390.00	$ 6,570.00
PB.FW.PaloAlto.PA3020.HA.NG.Base	Per device	$ 5,400.00	$ 6,570.00	0%	0%	$ 5,400.00	$ 6,570.00
PB.FW.PaloAlto.PA3050.HA.NG.Base	Per device	$ 8,440.00	$ 6,570.00	0%	0%	$ 8,440.00	$ 6,570.00
PB.FW.PaloAlto.PA5020.HA.NG.Base	Per device	$ 13,060.00	$ 6,570.00	0%	0%	$ 13,060.00	$ 6,570.00
PB.FW.PaloAlto.PA5050.HA.NG.Base	Per device	$ 22,350.00	$ 6,570.00	0%	0%	$ 22,350.00	$ 6,570.00

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.PaloAlto.PA5060.HA.NG.Base	Per device	$ 41,060.00	$ 6,570.00	0%	0%	$ 41,060.00	$ 6,570.00

STANDARD PBFW-NG OPTIONS - AVAILABLE ON ALL PLATFORMS

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.NG.URL	Per device	$ 160.00	0	0%	0%	$ 160.00	$ -
PB.FW.NG.TP	Per device	$ 780.00	0	0%	0%	$ 780.00	$ -
PB.FW.NG.ZD	Per device	$ 260.00	0	0%	0%	$ 260.00	$ -
PB.FW.OPT.ASI	Per device	$ 320.00	0	0%	0%	$ 320.00	$ -
PB.FW.OPT.CXE	Per device	$ 240.00	0	0%	0%	$ 240.00	$ -
PB.FW.OPT.S2S	Per device	$ 100.00	0	0%	0%	$ 100.00	$ -

NOTE: NG Bundles include the following Product Option Codes:

PB.FW.NG.URL

PB.FW.NG.TP

PB.FW.NG.ZD

AT&T Managed Security Services - Premises-Based Firewall - Small Business (SMB) Offers

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Fortinet.60.SBS.SA.LV1.50	Per device	$180.00	$230.00	0%	0%	$ 180.00	$ 230.00
PB.FW.Fortinet.60.SBS.SA.LV2.50	Per device	$290.00	$230.00	0%	0%	$ 290.00	$ 230.00

AT&T Managed Security Services - Premises-Based Firewall Service (PBFW) IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Fortinet.60.SBS.SA.LV3.50	Per device	$430.00	$230.00	0%	0%	$ 430.00	$ 230.00

OPTIONS - Charge is Per Tunnel

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.Fortinet.SBS.OPT.VPN	Per device	$40.00	$70.00	0%	0%	$ 40.00	$ 70.00

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.CheckPoint.2205.SBS.SA.500	Per device	$490.00	$2,590.00	0%	0%	$ 490.00	$ 2,590.00

OPTIONS

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.FW.OPT.ASI	Per device	$ 320.00	$ 2,000.00	0%	0%	$ 320.00	$ 2,000.00
PB.FW.OPT.S2S	Per device	$ 100.00	$ 540.00	0%	0%	$ 100.00	$ 540.00
PB.FW.OPT.C2S	Per device	$ 40.00	$ 670.00	0%	0%	$ 40.00	$ 670.00
PB.FW.OPT.CXE	Per device	$ 240.00	$ 2,000.00	0%	0%	$ 240.00	$ 2,000.00

AT&T Managed Intrusion Detection/Intrusion Prevention Service IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.IDPS.Sourcefire.3D7010.50.SA.CPR	Per device	$ 1,840.00	$ 5,540.00	0%	0%	$ 1,840.00	$ 5,540.00
PB.IDPS.Sourcefire.3D7020.100.SA.CPR	Per device	$ 2,100.00	$ 5,540.00	0%	0%	$ 2,100.00	$ 5,540.00
PB.IDPS.Sourcefire.3D7030.250.SA.CPR	Per device	$ 2,380.00	$ 5,660.00	0%	0%	$ 2,380.00	$ 5,660.00
PB.IDPS.Sourcefire.3D7110.500.SA.CPR	Per device	$ 3,340.00	$ 5,660.00	0%	0%	$ 3,340.00	$ 5,660.00
PB.IDPS.Sourcefire.3D7110.500.SA.FBR	Per device	$ 3,720.00	$ 5,660.00	0%	0%	$ 3,720.00	$ 5,660.00
PB.IDPS.Sourcefire.3D7120.1000.SA.CPR	Per device	$ 3,840.00	$ 5,800.00	0%	0%	$ 3,840.00	$ 5,800.00
PB.IDPS.Sourcefire.3D7120.1000.SA.FBR	Per device	$ 4,460.00	$ 5,800.00	0%	0%	$ 4,460.00	$ 5,800.00
PB.IDPS.Sourcefire.3D8120.2000.SA.CPR	Per device	$ 5,660.00	$ 5,920.00	0%	0%	$ 5,660.00	$ 5,920.00
PB.IDPS.Sourcefire.3D8120.2000.SA.FBR	Per device	$ 6,600.00	$ 5,920.00	0%	0%	$ 6,600.00	$ 5,920.00
PB.IDPS.Sourcefire.3D8130.4000.SA.CPR	Per device	$ 7,040.00	$ 5,920.00	0%	0%	$ 7,040.00	$ 5,920.00
PB.IDPS.Sourcefire.3D8130.4000.SA.FBR	Per device	$ 7,980.00	$ 5,920.00	0%	0%	$ 7,980.00	$ 5,920.00
PB.IDPS.Sourcefire.3D8140.6000.SA.CPR	Per device	$ 8,960.00	$ 5,920.00	0%	0%	$ 8,960.00	$ 5,920.00
PB.IDPS.Sourcefire.3D8140.6000.SA.FBR	Per device	$ 9,900.00	$ 5,920.00	0%	0%	$ 9,900.00	$ 5,920.00
PB.IDPS.McAfee.M1250.100.SA.CPR	Per device	$ 2,060.00	$ 5,540.00	0%	0%	$ 2,060.00	$ 5,540.00
PB.IDPS.McAfee.M1450.200.SA.CPR	Per device	$ 2,320.00	$ 5,660.00	0%	0%	$ 2,320.00	$ 5,660.00
PB.IDPS.McAfee.M2850.600.SA.CPR	Per device	$ 3,620.00	$ 5,660.00	0%	0%	$ 3,620.00	$ 5,660.00
PB.IDPS.McAfee.M2950.1000.SA.CPR	Per device	$ 4,280.00	$ 5,800.00	0%	0%	$ 4,280.00	$ 5,800.00
PB.IDPS.McAfee.M3050.1500.SA.CPR	Per device	$ 5,240.00	$ 5,920.00	0%	0%	$ 5,240.00	$ 5,920.00
PB.IDPS.McAfee.M4050.3000.SA.CPR	Per device	$ 7,740.00	$ 5,920.00	0%	0%	$ 7,740.00	$ 5,920.00
PB.IDPS.McAfee.M6050.5000.SA.CPR	Per device	$ 11,820.00	$ 5,920.00	0%	0%	$ 11,820.00	$ 5,920.00
PB.IDPS.TippingPoint.S110.100.SA.CPR	Per device	$ 2,020.00	$ 5,540.00	0%	0%	$ 2,020.00	$ 5,540.00
PB.IDPS.TippingPoint.S330.300.SA.CPR	Per device	$ 2,700.00	$ 5,660.00	0%	0%	$ 2,700.00	$ 5,660.00
PB.IDPS.TippingPoint.S660N.750.SA.CPR	Per device	$ 3,900.00	$ 5,660.00	0%	0%	$ 3,900.00	$ 5,660.00
PB.IDPS.TippingPoint.S1400N.1500.SA.CPR	Per device	$ 5,800.00	$ 5,920.00	0%	0%	$ 5,800.00	$ 5,920.00
PB.IDPS.TippingPoint.S2500N.3000.SA.CPR	Per device	$ 8,100.00	$ 5,920.00	0%	0%	$ 8,100.00	$ 5,920.00
PB.IDPS.TippingPoint.S5100N.5000.SA.CPR	Per device	$ 13,480.00	$ 5,920.00	0%	0%	$ 13,480.00	$ 5,920.00
PB.IDPS.Cisco.AIP-SSM10.50.SA.CPR.AIP	Per device	$ 1,480.00	$ 5,540.00	0%	0%	$ 1,480.00	$ 5,540.00
PB.IDPS.Cisco.AIP-SSM20.100.SA.CPR.AIP	Per device	$ 1,660.00	$ 5,540.00	0%	0%	$ 1,660.00	$ 5,540.00
PB.IDPS.Cisco.4240.250.SA.CPR	Per device	$ 1,900.00	$ 5,660.00	0%	0%	$ 1,900.00	$ 5,660.00
PB.IDPS.Cisco.4255.500.SA.CPR	Per device	$ 2,480.00	$ 5,660.00	0%	0%	$ 2,480.00	$ 5,660.00
PB.IDPS.Cisco.4260.1000.SA.CPR	Per device	$ 3,060.00	$ 5,800.00	0%	0%	$ 3,060.00	$ 5,800.00

AT&T Managed Intrusion Detection/Intrusion Prevention Service IaaS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.IDPS.Cisco.4270.2000.SA.CPR	Per device	$ 4,640.00	$ 5,920.00	0%	0%	$ 4,640.00	$ 5,920.00

STANDARD MIDPS OPTIONS - AVAILABLE ON ALL PLATFORMS

Product Code	Units	List MRC	List OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.IDPS.OPT.ETS	Per device	$ 760.00	$ 1,580.00	0%	0%	$ 760.00	$ 1,580.00

AT&T Managed Security Services - Managed Host-Based Intrusion Detection/Prevention Services Offers

Product Code	Units	MRC	OTC	MRC Discount	OTC Discount	Net MRC	Net OTC
PB.IDPS.McAfee.HIDS.HIPS	Per device	$ 190.00	$ 250.00	0%	0%	$ 190.00	$ 250.00
PB.IDPS.McAfee.HIDS.HIPS.CC	Per device	$ 220.00	$ 250.00	0%	0%	$ 220.00	$ 250.00
PB.IDPS.McAfee.HIDS.AC	Per device	$ 190.00	$ 250.00	0%	0%	$ 190.00	$ 250.00
PB.IDPS.McAfee.HIDS.CC	Per device	$ 200.00	$ 250.00	0%	0%	$ 200.00	$ 250.00
PB.IDPS.McAfee.HIDS.AC.CC	Per device	$ 220.00	$ 250.00	0%	0%	$ 220.00	$ 250.00

AT&T Professional Services IaaS

Product or Service Orderable Items			List Price	List Price	NASPO Discount		Net Price	Net Price
Component	Description	Units	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
AT&T Cloud Professional Services – Project Fees								
Cloud Solution Planning Workshop								
Cloud Solution Planning Workshop	Level-of-Effort, assumed duration of 2 weeks**includes	Fee	$20,000	$ -	0%	0%	$ 20,000.00	$ -
Cloud Strategy and Roadmap								
Cloud Strategy and Roadmap	Level of Effort: Small	Fee	$200,000	$ -	0%	0%	$ 200,000.00	$ -
Cloud Strategy and Roadmap	Level of Effort: Medium	Fee	$350,000	$ -	0%	0%	$ 350,000.00	$ -
Cloud Strategy and Roadmap	Level of Effort: Large	Fee	$500,000	$ -	0%	0%	$ 500,000.00	$ -
Cloud Implementation and Governance								
Cloud Implementation and Governance	Level of Effort: Small	Fee	$100,000	$ -	0%	0%	$ 100,000.00	$ -
Cloud Implementation and Governance	Level of Effort: Medium	Fee	$150,000	$ -	0%	0%	$ 150,000.00	$ -
Cloud Implementation and Governance	Level of Effort: Large	Fee	$200,000	$ -	0%	0%	$ 200,000.00	$ -
Cloud Security and Compliance Assessment								
Cloud Security and Compliance Assessment	Level of Effort: Small	Fee	$50,000	$ -	0%	0%	$ 50,000.00	$ -
Cloud Security and Compliance Assessment	Level of Effort: Medium	Fee	$75,000	$ -	0%	0%	$ 75,000.00	$ -
Cloud Security and Compliance Assessment	Level of Effort: Large	Fee	$100,000	$ -	0%	0%	$ 100,000.00	$ -
Subtotal	*AT&T Cloud Professional Services – Project Fees*							

Notes:

AT&T prices our services for a given consulting project based on the estimated man-hours/ Level-of-Effort (LOE) of the consultants assigned to the project, software tools, and engagement management for quality assurance. Factors that affect our Level-of-Effort estimate include: required number of interviews, complexity of cloud solution alternatives to be analyzed, number of applications, number of data centers, number of servers, size of network, diversity of technologies etc.

Based on our experience with other government agencies, however, we have created standard project fees based on an assumed Level-of-Effort for different agency/project sizes under this RFP for each of the categories of services listed below.

Cloud Solution Planning Workshop

AT&T's on-site Cloud Solution Planning Workshop helps clients determine where opportunities may exist to benefit from cloud services. Typically, during a Cloud Solution Planning Workshop we work with you to:

- Establish a vision for cloud services relevant to your business and its goals
- Review common industry use cases
- Discuss relevant business requirements / IT imperatives
- Identify target applications / services for cloud strategy and business case development
- Establish next steps for your Cloud Strategy development or Implementation

Level-of-Effort

2 weeks* *includes custom preparation/research, 1-2 day on-site workshop, and findings report preparation

Cloud Strategy and Roadmap

AT&T Professional Services IaaS

Product or Service Orderable Items			List Price	List Price	NASPO Discount		Net Price	Net Price
Component	Description	Units	Unit NRC	Unit MRC	NRC Discount	MRC Discount	Unit NRC	Unit MRC
AT&T Cloud Professional Services – Project Fees								
Cloud Solution Planning Workshop								
Cloud Solution Planning Workshop	Level-of-Effort, assumed duration of 2 weeks**includes	Fee	$20,000	$ -	0%	0%	$ 20,000.00	$ -
Cloud Strategy and Roadmap								
Cloud Strategy and Roadmap	Level of Effort: Small	Fee	$200,000	$ -	0%	0%	$ 200,000.00	$ -
Cloud Strategy and Roadmap	Level of Effort: Medium	Fee	$350,000	$ -	0%	0%	$ 350,000.00	$ -
Cloud Strategy and Roadmap	Level of Effort: Large	Fee	$500,000	$ -	0%	0%	$ 500,000.00	$ -
Cloud Implementation and Governance								
Cloud Implementation and Governance	Level of Effort: Small	Fee	$100,000	$ -	0%	0%	$ 100,000.00	$ -
Cloud Implementation and Governance	Level of Effort: Medium	Fee	$150,000	$ -	0%	0%	$ 150,000.00	$ -
Cloud Implementation and Governance	Level of Effort: Large	Fee	$200,000	$ -	0%	0%	$ 200,000.00	$ -
Cloud Security and Compliance Assessment								
Cloud Security and Compliance Assessment	Level of Effort: Small	Fee	$50,000	$ -	0%	0%	$ 50,000.00	$ -
Cloud Security and Compliance Assessment	Level of Effort: Medium	Fee	$75,000	$ -	0%	0%	$ 75,000.00	$ -
Cloud Security and Compliance Assessment	Level of Effort: Large	Fee	$100,000	$ -	0%	0%	$ 100,000.00	$ -
Subtotal	*AT&T Cloud Professional Services – Project Fees*							

Notes:

AT&T prices our services for a given consulting project based on the estimated man-hours/ Level-of-Effort (LOE) of the consultants assigned to the project, software tools, and engagement management for quality assurance. Factors that affect our Level-of-Effort estimate include: required number of interviews, complexity of cloud solution alternatives to be analyzed, number of applications, number of data centers, number of servers, size of network, diversity of technologies etc.

Based on our experience with other government agencies, however, we have created standard project fees based on an assumed Level-of-Effort for different agency/project sizes under this RFP for each of the categories of services listed below.

Cloud Solution Planning Workshop

AT&T's on-site Cloud Solution Planning Workshop helps clients determine where opportunities may exist to benefit from cloud services. Typically, during a Cloud Solution Planning Workshop we work with you to:

- Establish a vision for cloud services relevant to your business and its goals
- Review common industry use cases
- Discuss relevant business requirements / IT imperatives
- Identify target applications / services for cloud strategy and business case development
- Establish next steps for your Cloud Strategy development or Implementation

Level-of-Effort

2 weeks* *includes custom preparation/research, 1-2 day on-site workshop, and findings report preparation

Cloud Strategy and Roadmap

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
Ion Standard						
Ion Standard	***Notes:***					
	Ion Standard includes: 1 Web Experience, 5 GB NetStorage, 1,000 Million Hits of Adaptive Image Compression*, & 200 Site Analyzer tokens (per contract term). Page Weight Cap is added for MPV pricing (400 GB of delivery is included per MPV committed; additional charges are added if this allowance is exceeded). Commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied. *Adaptive Image Compression is selected by default in Apttus and Momentum when Ion Standard orders are created. Please note that the product must be specified on the order form for the customer to gain access to the product in Luna.					
Ion Standard	***Platform Fee:***					
			Monthly			4,825.00
Ion Standard	***Included:***					
	Web Experiences:					
		Web Experiences	Monthly	1		
	NetStorage:					
		GB Stored	Monthly	5		
	Site Analyzer:					
		Tokens	Per Contract	200		
	Adaptive Image Compression:					
		Million Hits	Monthly	1000		
Ion Standard	***Usage:***					
Ion Standard	***GB - Commitment:***					
		GB	Monthly	0	2,000	1.02
		GB	Monthly	2,001	6,000	0.95
		GB	Monthly	6,001	15,000	0.86
		GB	Monthly	15,001	30,000	0.71
		GB	Monthly	30,001	50,000	0.63
		GB	Monthly	50,001	100,000	0.55
		GB	Monthly	100,001	150,000	0.51
		GB	Monthly	150,001	999,999,999	0.42

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	GB - Overage:					
		GB	As Incurred	0	2,000	1.12
		GB	As Incurred	2,001	6,000	1.05
		GB	As Incurred	6,001	15,000	0.95
		GB	As Incurred	15,001	30,000	0.78
		GB	As Incurred	30,001	50,000	0.69
		GB	As Incurred	50,001	100,000	0.62
		GB	As Incurred	100,001	150,000	0.55
		GB	As Incurred	150,001	999,999,999	0.46
Ion Standard	***Additional Options:***					
	Site Analyzer (min of 10):					
		Tokens	Per Contract	10	999,999,999	35.00
	Adaptive Image Compression:					
		Million Hits	Monthly	1,000	999,999,999	50.00
	Adaptive Image Compression - Overage:					
		Million Hits	Monthly	1,000	999,999,999	50.00
	Web Experiences:					
		Web Experiences	Monthly	1	999,999,999	1,000.00
Ion Standard	***Standard Intergration Fees:***					
	Ion Standard - Standard Integration New Customer:					
			One-Time			9,000.00
	Ion Standard - Standard Integration from DSD:					
			One-Time			6,000.00
	Ion Standard - Standard Integration from DSA, RMA:					
			One-Time			4,500.00
	Ion Standard - Standard Integration from DSA-P:					
			One-Time			2,500.00
Ion Standard	***Managed Intergration Fees:***					
	Ion Standard - Managed Integration New Customer:					
			One-Time			20,000.00
	Ion Standard - Managed Integration from DSD:					
			One-Time			6,000.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Ion Standard - Managed Integration from DSA, RMA:					
			One-Time			4,500.00
Ion Standard w/ HTTPS Option						
Ion Std. HTTPS	***Notes:***					
	Ion Standard w/ HTTPS Option includes: 1 Web Experience, 5 GB NetStorage, 1,000 Million Hits of Adaptive Image Compression*, 200 Site Analyzer tokens (per contract term), 1 Certificate: Choice of Single hostname, SAN, EV Single hostname or Wildcard. Page Weight Cap is added for MPV pricing (400 GB of delivery is included per MPV committed; additional charges are added if this allowance is exceeded). Commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied. *Adaptive Image Compression is selected by default in Apttus and Momentum when Ion Standard orders are created. Please note that the product must be specified on the order form for the customer to gain access to the product in Luna.					
Ion Std. HTTPS	***Platform Fee:***					
			Monthly			6,750.00
Ion Std. HTTPS	***Included:***					
	Web Experiences:					
		Web Experiences	Monthly	1		
	SSL Network Access (SAN or Wildcard Cert):					
		Certificate	Monthly	1		
	NetStorage:					
		GB Stored	Monthly	5		
	Site Analyzer:					
		Tokens	Per Contract	200		
	Adaptive Image Compression:					
		Million Hits	Monthly	1,000		
	Page Weight Cap (MPV Only):					
		GB/MPV	Monthly	400		
	SSL Network Access-Extended Validation					
		Certificate	Monthly	1		

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
Ion Std. HTTPS	***Usage:***					
Ion Std. HTTPS	***GB - Commitment:***					
		GB	Monthly	0	2,000	1.26
		GB	Monthly	2,001	6,000	1.18
		GB	Monthly	6,001	15,000	1.06
		GB	Monthly	15,001	30,000	0.89
		GB	Monthly	30,001	50,000	0.78
		GB	Monthly	50,001	100,000	0.71
		GB	Monthly	100,001	150,000	0.63
		GB	Monthly	150,001	999,999,999	0.52
	GB - Overage:					
		GB	As Incurred	0	2,000	1.38
		GB	As Incurred	2,001	6,000	1.31
		GB	As Incurred	6,001	15,000	1.17
		GB	As Incurred	15,001	30,000	0.98
		GB	As Incurred	30,001	50,000	0.86
		GB	As Incurred	50,001	100,000	0.78
		GB	As Incurred	100,001	150,000	0.69
		GB	As Incurred	150,001	999,999,999	0.57
Ion Std. HTTPS	***Additional Options:***					
	Site Analyzer (min of 10):					
		Tokens	Per Contract	10	999,999,999	35.00
	Adaptive Image Compression:					
		Million Hits	Monthly	1,000	999,999,999	50.00
	Adaptive Image Compression - Overage:					
		Million Hits	Monthly	1,000	999,999,999	50.00
	Web Experiences:					
		Web Experiences	Monthly	1	999,999,999	1,000.00
Ion Std. HTTPS	***Standard Intergration Fees:***					
	Ion Standard - Standard Integration New Customer:					
			One-Time			9,000.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Ion Standard - Standard Integration from DSD:					
			One-Time			6,000.00
	Ion Standard - Standard Integration from DSA, RMA:					
			One-Time			4,500.00
Ion Std. HTTPS	***Managed Intergration Fees:***					
	Ion Standard - Managed Integration New Customer:					
			One-Time			20,000.00
	Ion Standard - Managed Integration from DSD:					
			One-Time			10,000.00
	Ion Standard - Managed Integration from DSA, RMA:					
			One-Time			6,000.00
Dynamic Site Accelerator						
DSA	***Notes:***					

Dynamic Site Accelerator includes: 1 Web Experience, 5 GB NetStorage, & 200 Site Analyzer tokens (per contract term). Page Weight Cap is added for MPV pricing (400 GB of delivery is included per MPV committed; additional charges are added if this allowance is exceeded). Commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied.

Please note : Legacy Shopper Prioritization will only be available to renewals and not on new contracts. Cloudlet replacement will be used for new contracts.

DSA	***Base Fee:***					
			Monthly			2,923.08
DSA	***Included:***					
	Web Experiences:					
		Web Experiences	Monthly		1	
	NetStorage:					
		GB Stored	Monthly		5	
	Site Analyzer:					
		Tokens	Per Contract		200	

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
DSA	***Usage:***					
DSA	***GB - Commitment:***					
		GB	Monthly	0	2,000	0.62
		GB	Monthly	2,001	6,000	0.62
		GB	Monthly	6,001	15,000	0.62
		GB	Monthly	15,001	30,000	0.62
		GB	Monthly	30,001	50,000	0.62
		GB	Monthly	50,001	100,000	0.46
		GB	Monthly	100,001	150,000	0.38
		GB	Monthly	150,001	250,000	0.35
		GB	Monthly	250,001	500,000	0.28
		GB	Monthly	500,001	999,999,999	0.20
	GB - Overage:					
		GB	As Incurred	0	2,000	0.62
		GB	As Incurred	2,001	6,000	0.62
		GB	As Incurred	6,001	15,000	0.62
		GB	As Incurred	15,001	30,000	0.62
		GB	As Incurred	30,001	50,000	0.62
		GB	As Incurred	50,001	100,000	0.46
		GB	As Incurred	100,001	150,000	0.38
		GB	As Incurred	150,001	250,000	0.35
		GB	As Incurred	250,001	500,000	0.28
		GB	As Incurred	500,001	999,999,999	0.20
Dynamic Site Accelerator w/HTTPS Option						
DSA	***Notes:***					

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Dynamic Site Accelerator w/ HTTPS Option includes: 1 Web Experience, 5 GB NetStorage, 200 Site Analyzer tokens (per contract term), 1 Certificate: Choice of Single hostname, SAN, EV Single hostname or Wildcard. Page Weight Cap is added for MPV pricing (400 GB of delivery is included per MPV committed; additional charges are added if this allowance is exceeded). Commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied. ***Please note:*** Legacy Shopper Prioritization will only be available to renewals and not on new contracts. Cloudlet replacement will be used for new contracts.					
DSA	***Base Fee:***					
			Monthly			4,461.54
DSA	***Included:***					
	Web Experiences:					
		Web Experiences	Monthly		1	
	NetStorage:					
		GB Stored	Monthly		5	
	Site Analyzer:					
		Tokens	Per Contract		200	
DSA	***Usage:***					
DSA	***GB - Commitment:***					
		GB	Monthly	0	2,000	0.72
		GB	Monthly	2,001	6,000	0.72
		GB	Monthly	6,001	15,000	0.72
		GB	Monthly	15,001	30,000	0.72
		GB	Monthly	30,001	50,000	0.72
		GB	Monthly	50,001	100,000	0.55
		GB	Monthly	100,001	150,000	0.46
		GB	Monthly	150,001	250,000	0.42
		GB	Monthly	250,001	500,000	0.32

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		GB	Monthly	500,001	999,999,999	0.23
	GB - Overage:					
		GB	As Incurred	0	2,000	0.72
		GB	As Incurred	2,001	6,000	0.72
		GB	As Incurred	6,001	15,000	0.72
		GB	As Incurred	15,001	30,000	0.72
		GB	As Incurred	30,001	50,000	0.72
		GB	As Incurred	50,001	100,000	0.55
		GB	As Incurred	100,001	150,000	0.46
		GB	As Incurred	150,001	250,000	0.42
		GB	As Incurred	250,001	500,000	0.32
		GB	As Incurred	500,001	999,999,999	0.23
Adaptive Media Delivery						
AMD	***Notes:***					
	Adaptive Media Delivery includes 5,000 GB of usage. There is no included traffic if the Mbps commit model is used. Additional commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied.					
AMD	***Base Fee:***					
			Monthly			1,332.00
AMD	***Included:***					
	GB Traffic					
		GB	Monthly	5,000		
AMD	***Usage:***					
AMD	***GB - Commitment:***					
		GB	Monthly	0	10,000	0.2770
		GB	Monthly	10,001	25,000	0.2230
		GB	Monthly	25,001	50,000	0.1260

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	GB	Monthly	50,001	100,000	0.1040
	GB	Monthly	100,001	250,000	0.0860
	GB	Monthly	250,001	500,000	0.0670
	GB	Monthly	500,001	1,000,000	0.0490
	GB	Monthly	1,000,001	2,500,000	0.0320
	GB	Monthly	2,500,001	999,999,999	0.0310
GB - Overage:					
	GB	As Incurred	0	10,000	0.2770
	GB	As Incurred	10,001	25,000	0.2230
	GB	As Incurred	25,001	50,000	0.1260
	GB	As Incurred	50,001	100,000	0.1040
	GB	As Incurred	100,001	250,000	0.0860
	GB	As Incurred	250,001	500,000	0.0670
	GB	As Incurred	500,001	1,000,000	0.0490
	GB	As Incurred	1,000,001	2,500,000	0.0320
	GB	As Incurred	2,500,001	999,999,999	0.0310

Media Services - Live

MS - Live ***Notes:***

Media Services Live includes ingestion as a tiered base fee based on the estimated number of minutes the customer expects to ingest monthly. NOTE: The below fees are NOT per unit; they are flat base fees. The below tiers are guidelines for sales to derive the appropriate base fee for the customer. At launch, MS-L will not track actual usage nor will invoices reflect actual usage.

MS - Live ***Base Fee:***

Media Services - Live - Base Fee:					
	Minutes	Monthly	1	10,000	960.00
	Minutes	Monthly	10,001	30,000	1,500.00
	Minutes	Monthly	30,001	250,000	3,600.00

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Minutes	Monthly	250,001	500,000	6,000.00
	Minutes	Monthly	500,001	1,000,000	10,800.00
	Minutes	Monthly	1,000,001	5,000,000	15,000.00
	Minutes	Monthly	5,000,001	999,999,999	19,500.00

Media Services - Live / Stream Packaging

MS-Live/Strm Pkg. ***Notes:***

Stream Packaging is an option MS-L customers can add, it includes pricing tiers for Video and Audio Only. Media Services Live bills Stream Packaging as a base fee based on the estimated number of minutes the customer expects to package monthly. NOTE: The below fees are NOT per unit; they are flat base fees. The below tiers are guidelines for sales to derive the appropriate base fee for the customer. At launch, MS-L will not track actual usage nor will invoices reflect actual usage.

MS-Live/Strm Pkg. ***Base Fee:***

Media Services - Live/ Stream Packaging - Base Fee:

	Minutes	Monthly	1	10,000	3,200.00
	Minutes	Monthly	10,001	30,000	5,000.00
	Minutes	Monthly	30,001	250,000	12,000.00
	Minutes	Monthly	250,001	500,000	20,000.00
	Minutes	Monthly	500,001	1,000,000	36,000.00
	Minutes	Monthly	1,000,001	5,000,000	50,000.00
	Minutes	Monthly	5,000,001	999,999,999	65,000.00

Media Services - Live/ Stream Packaging - Base Fee (AUDIO ONLY):

	Minutes	Monthly	1	10,000	320.00
	Minutes	Monthly	10,001	30,000	500.00
	Minutes	Monthly	30,001	250,000	1,700.00
	Minutes	Monthly	250,001	500,000	2,000.00
	Minutes	Monthly	500,001	1,000,000	3,600.00
	Minutes	Monthly	1,000,001	5,000,000	5,000.00
	Minutes	Monthly	5,000,001	999,999,999	6,500.00

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
Media Services - On Demand / Stream Packaging					
MSOD - Strm Pkg.	***Notes:***				
	The below fees are NOT per unit; they are flat base fees. The below tiers are guidelines for sales to derive the appropriate base fee for the customer. At launch, MSOD will not track actual usage nor will invoices reflect actual usage. The unit of measure for the tiers is GBs Prepared				
MSOD - Strm Pkg.	***Base Fee:***				
	Media Services - On Demand/ Stream Packaging - Base Fee:				
	GB Prepared	Monthly	0	200	3,200.00
	GB Prepared	Monthly	201	400	5,000.00
	GB Prepared	Monthly	401	1,000	12,000.00
	GB Prepared	Monthly	1,001	2,000	20,000.00
	GB Prepared	Monthly	2,001	5,000	45,000.00
	GB Prepared	Monthly	5,001	10,000	50,000.00
	GB Prepared	Monthly	10,001	999,999,999	65,000.00
	Media Services - On Demand/ Stream Packaging - Base Fee (AUDIO ONLY):				
	GB Prepared	Monthly	0	200	320.00
	GB Prepared	Monthly	201	400	500.00
	GB Prepared	Monthly	401	1,000	1,700.00
	GB Prepared	Monthly	1,001	2,000	2,000.00
	GB Prepared	Monthly	2,001	5,000	4,500.00
	GB Prepared	Monthly	5,001	10,000	5,000.00
	GB Prepared	Monthly	10,001	999,999,999	6,500.00
NetStorage					
NetStorage	***Notes:***				
	Commitments are priced per unit. If the customer exceeds their commitment, an overage charge is applied. Aspera is a mandatory option with NetStorage as of Jan 2015.				

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
NetStorage	***Usage:***					
NetStorage	***GB Stored - Commitment:***					
		GB Stored	Monthly	0	2,500	1.70
		GB Stored	Monthly	2,501	5,000	1.19
		GB Stored	Monthly	5,001	10,000	0.68
		GB Stored	Monthly	10,001	25,000	0.51
		GB Stored	Monthly	25,001	50,000	0.46
		GB Stored	Monthly	50,001	100,000	0.39
		GB Stored	Monthly	100,001	250,000	0.31
		GB Stored	Monthly	250,001	500,000	0.27
		GB Stored	Monthly	500,001	999,999,999	0.20
	GB Stored - Overage:					
		GB Stored	As Incurred	0	2,500	1.70
		GB Stored	As Incurred	2,501	5,000	1.19
		GB Stored	As Incurred	5,001	10,000	0.68
		GB Stored	As Incurred	10,001	25,000	0.51
		GB Stored	As Incurred	25,001	50,000	0.46
		GB Stored	As Incurred	50,001	100,000	0.39
		GB Stored	As Incurred	100,001	250,000	0.31
		GB Stored	As Incurred	250,001	500,000	0.27
		GB Stored	As Incurred	500,001	999,999,999	0.20
	Aspera Pay as You Go (This is a mandatory option with NetStorage as of Jan 2015):					
		GB Stored	Monthly	0	999,999,999	0.10

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
Content Targeting						
Content Targeting	***Base Fee:***					
			Monthly			750.00
SSL Network Access						
SSL Access	***Notes:***					
	Additional SSL certs can be purchased per unit based on the prices below.					
SSL Access	***Base Fee:***					
	SSL Network Access - Single Hostname:					
		Certificate	Monthly			425.00
	SSL Network Access - Extended Validation:					
		Certificate	Monthly			562.50
	SSL Network Access - Extended Validation SAN:					
		Certificate	Monthly			1,250.00
	SSL Network Access - Wildcard:					
		Certificate	Monthly			425.00
	SSL Network Access - 3rd Party:					
		Certificate	Monthly			312.50
	SSL Network Access - SAN:					
		Certificate	Monthly			625.00
Fast DNS - Standalone						
Fast DNS - Stand	***Notes:***					
	A customer buys support for a certain number of zones by selecting the appropriate plan. Additional zones can be purchased; however, the rate per additional zone varies depending on the plan selected. For example: To purchase 8 zones, a customer should purchase the 3 zone plan for $750 and 5 additional zones @ $150 per zones. The Secure Option fee is ***in addition to*** the base fee. The Secure Option fee will vary depending on the plan selected.					
Fast DNS - Stand	***Plan Fee:***			**Plan**	**Incl. Amount**	
	Fast DNS - Base Plan:					
		Zones	Monthly	3 Zone Plan	3	750.00

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Zones	Monthly	10 Zone Plan	10	1,500.00
	Zones	Monthly	50 Zone Plan	50	3,750.00
	Zones	Monthly	100 Zone Plan	100	5,250.00
Fast DNS - Additional Zones (Prices are per Zone):					
	Zones	Monthly	3 Zone Plan		150.00
	Zones	Monthly	10 Zone Plan		60.00
	Zones	Monthly	50 Zone Plan		37.50
	Zones	Monthly	100 Zone Plan		4.50

Fast DNS - Stand	*Secure Option:*		Plan		
	Fast DNS - Secure Option (this fee is added to the Base Fee):				
	Zones	Monthly	3 Zone Plan		750.00
	Zones	Monthly	10 Zone Plan		1,500.00
	Zones	Monthly	50 Zone Plan		3,750.00
	Zones	Monthly	100 Zone Plan		5,250.00

Global Traffic Management - Standard

GTM - Standard	*Notes:*

A customer buys support for a certain number of properties by selecting the appropriate plan. Additional properties can be purchased; however, the rate per additional property varies depending on the plan selected. For example: To purchase 8 properties, a customer should purchase the 5 property plan for $3,3750 and 3 additional properties @ $150 per property.

GTM - Standard	*Plan Fee:*		Plan	Incl. Amount	
	Global Traffic Management - Standard - Base Plan:				
	Properties	Monthly	2 Property Plan	2	750.00
	Properties	Monthly	5 Property Plan	5	1,500.00
	Properties	Monthly	20 Property Plan	20	3,000.00
	Properties	Monthly	50 Property Plan	50	4,500.00
Global Traffic Management - Standard - Additional Properties (Prices are per Property):					

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Properties	Monthly	2 Property Plan		300.00
	Properties	Monthly	5 Property Plan		150.00
	Properties	Monthly	20 Property Plan		60.00
	Properties	Monthly	50 Property Plan		15.00

Global Traffic Management - Premier

GTM - Premier ***Notes:***

A customer buys support for a certain number of properties by selecting the appropriate plan. Additional properties can be purchased; however, the rate per additional property varies depending on the plan selected. For example: To purchase 8 properties, a customer should purchase the 5 property plan for $3,3750 and 3 additional properties @ $150 per property.

GTM - Premier	*Plan Fee:*		Plan	Incl. Amount	
	Global Traffic Management - Premier - Base Plan:				
	Properties	Monthly	2 Property Plan	2	2,250.00
	Properties	Monthly	5 Property Plan	5	3,750.00
	Properties	Monthly	20 Property Plan	20	7,500.00
	Properties	Monthly	50 Property Plan	50	11,250.00
	Global Traffic Management - Premier - Additional Properties (Prices are per Property):				
	Properties	Monthly	2 Property Plan		750.00
	Properties	Monthly	5 Property Plan		375.00
	Properties	Monthly	20 Property Plan		150.00
	Properties	Monthly	50 Property Plan		37.50

Kona Site Defender

KSD ***Notes:***

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail

Kone Site Defender can be orderd in either Mbps or GB. The included amount (Mbps or GB) is based on the plan 'tier' selected for the Base Fee. The plan includes one site OR one application. Customer can add any number of sites and/or applications in combination. Kona Site Defender entitles the customer to two Policies and one Site Shield map. Customers have the option to add additional Policies or Site Shield maps. Includes DDoS Fee Protection with capped burst fee of $5,000 as incurred per month.

KSD	***Included:***					
	Sites or Applications (choose one):					
		Sites or Applications	Contract Term	1		
	Policies:					
		Policies	Contract Term	2		
	Site Shield Maps:					
		Maps	Contract Term	1		
	DDoS Fee Protection:					
			Contract Term	n/a		
KSD	***Base Fee:***			**Plan**	**Incl. Amount**	
KSD	***GB - Plans:***					
		GB	Monthly	7,500 GB Plan	7,500	8,800.00
		GB	Monthly	15,000 GB Plan	15,000	11,600.00
		GB	Monthly	30,000 GB Plan	30,000	14,000.00
		GB	Monthly	45,000 GB Plan	45,000	16,000.00
		GB	Monthly	75,000 GB Plan	75,000	18,000.00
		GB	Monthly	105,000 GB Plan	105,000	20,000.00
		GB	Monthly	150,000 GB Plan	150,000	22,000.00
		GB	Monthly	300,000 GB Plan	300,000	26,000.00
	GB - Overage (prices are per GB):					
		GB	As Incurred	7,500 GB Plan		0.60
		GB	As Incurred	15,000 GB Plan		0.56

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		GB	As Incurred	30,000 GB Plan		0.52
		GB	As Incurred	45,000 GB Plan		0.48
		GB	As Incurred	75,000 GB Plan		0.42
		GB	As Incurred	105,000 GB Plan		0.37
		GB	As Incurred	150,000 GB Plan		0.30
		GB	As Incurred	300,000 GB Plan		0.24
KSD	***Additional Fees & Options:***					
	Capped burst fee:					
			As Incurred			0.00
	Sites:					
		Sites	Monthly	1	10	400.00
		Sites	Monthly	11	20	280.00
		Sites	Monthly	21	50	200.00
		Sites	Monthly	51	100	160.00
		Sites	Monthly	101	200	120.00
	Applications:					
		Applications	Monthly	1	5	1,600.00
		Applications	Monthly	6	10	1,440.00
		Applications	Monthly	11	20	1,280.00
		Applications	Monthly	21	50	1,120.00
		Applications	Monthly	51	100	960.00
	Policies:					
		Policies	Monthly	1	999,999,999	1,600.00
	Additional Site Shield Maps:					
		GB	Monthly	7,500 GB Plan		2,495.00
		GB	Monthly	15,000 GB Plan		3,288.60
		GB	Monthly	30,000 GB Plan		3,969.00
		GB	Monthly	45,000 GB Plan		4,536.00
		GB	Monthly	75,000 GB Plan		5,103.00
		GB	Monthly	105,000 GB Plan		5,670.00

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	GB	Monthly	150,000 GB Plan		6,237.00
	GB	Monthly	300,000 GB Plan		7,371.00
HTTPS Option (includes 1 Certificate; Choice of SAN or Wildcard):					
	GB	Monthly	7,500 GB Plan		3,520.00
	GB	Monthly	15,000 GB Plan		4,640.00
	GB	Monthly	30,000 GB Plan		5,600.00
	GB	Monthly	45,000 GB Plan		6,400.00
	GB	Monthly	75,000 GB Plan		7,200.00
	GB	Monthly	105,000 GB Plan		8,000.00
	GB	Monthly	150,000 GB Plan		8,800.00
	GB	Monthly	300,000 GB Plan		10,400.00
On Site Audit:					
		One Time			40,000.00

Web Application Firewall

WAF	***Notes:***				

WAF can be orderd in either Mbps or GB. The included amount (Mbps or GB) is based on the plan 'tier' selected for the Base Fee. A minimum of one site or application must be selected. Customer can add any number of sites and/or applications in combination. WAF entitles the customer to two Policies.

WAF	***Included:***				
	Sites or Applications (choose one):				
		Sites or Applications	Contract Term	1	
	Policies:				
		Policies	Contract Term	2	

WAF	***Base Fee:***			Plan	Incl. Amount	
WAF	***GB - Plans:***					
		GB	Monthly	7,500 GB Plan	7,500	5,720.00
		GB	Monthly	15,000 GB Plan	15,000	7,540.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		GB	Monthly	30,000 GB Plan	30,000	9,100.00
		GB	Monthly	45,000 GB Plan	45,000	10,400.00
		GB	Monthly	75,000 GB Plan	75,000	11,700.00
		GB	Monthly	105,000 GB Plan	105,000	13,000.00
		GB	Monthly	150,000 GB Plan	150,000	14,300.00
		GB	Monthly	300,000 GB Plan	300,000	16,900.00
	GB - Overage (prices are per GB):					
		GB	As Incurred	7,500 GB Plan		0.39
		GB	As Incurred	15,000 GB Plan		0.36
		GB	As Incurred	30,000 GB Plan		0.34
		GB	As Incurred	45,000 GB Plan		0.31
		GB	As Incurred	75,000 GB Plan		0.28
		GB	As Incurred	105,000 GB Plan		0.24
		GB	As Incurred	150,000 GB Plan		0.20
		GB	As Incurred	300,000 GB Plan		0.16
WAF	***Additional Fees & Options:***					
	Sites:					
		Sites	Monthly	1	10	320.00
		Sites	Monthly	11	20	260.00
		Sites	Monthly	21	50	200.00
		Sites	Monthly	51	100	140.00
		Sites	Monthly	101	200	64.00
	Applications:					
		Applications	Monthly	1	5	1,280.00
		Applications	Monthly	6	10	1,152.00
		Applications	Monthly	11	20	1,024.00
		Applications	Monthly	21	50	896.00
		Applications	Monthly	51	100	768.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Policies:					
		Policies	Monthly	1	999,999,999	1,600.00
Site Shield						
Site Shield	***Notes:***					
	Site Shield can be orderd in either Mbps or GB. The included amount (Mbps or GB) is based on the plan 'tier' selected for the Base Fee. Primary Site Shield entitles the customer to one Site Shield map.					
Site Shield	***Included:***					
	Site Shield Maps:					
		Maps	Contract Term	1		
Site Shield	***Base Fee:***			**Plan**	**Incl. Amount**	
Site Shield	***GB - Plans:***					
		GB	Monthly	7,500 GB Plan	7,500	3,240.00
		GB	Monthly	15,000 GB Plan	15,000	5,220.00
		GB	Monthly	30,000 GB Plan	30,000	6,300.00
		GB	Monthly	45,000 GB Plan	45,000	7,200.00
		GB	Monthly	75,000 GB Plan	75,000	8,100.00
		GB	Monthly	105,000 GB Plan	105,000	9,000.00
		GB	Monthly	150,000 GB Plan	150,000	9,900.00
		GB	Monthly	300,000 GB Plan	300,000	11,700.00
	GB - Overage (prices are per GB):					
		GB	As Incurred	7,500 GB Plan		0.27
		GB	As Incurred	15,000 GB Plan		0.25
		GB	As Incurred	30,000 GB Plan		0.23
		GB	As Incurred	45,000 GB Plan		0.22
		GB	As Incurred	75,000 GB Plan		0.19

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		GB	As Incurred	105,000 GB Plan		0.17
		GB	As Incurred	150,000 GB Plan		0.14
		GB	As Incurred	300,000 GB Plan		0.11
Site Shield	***Additional Fees & Options:***					
	Additional Site Shield Maps:					
		GB	Monthly	7,500 GB Plan		2,268.00
		GB	Monthly	15,000 GB Plan		3,654.00
		GB	Monthly	30,000 GB Plan		4,410.00
		GB	Monthly	45,000 GB Plan		5,040.00
		GB	Monthly	75,000 GB Plan		5,670.00
		GB	Monthly	105,000 GB Plan		6,300.00
		GB	Monthly	150,000 GB Plan		6,930.00
		GB	Monthly	300,000 GB Plan		8,190.00
Client Reputation						
Client Reputation	***Notes:***					

Client Reputation can be orderd in either Mbps or GB. The included amount (Mbps or GB) is based on the plan 'tier' selected for the Base Fee.

				Plan	Incl. Amount	
Client Reputation	***Base Fee:***					
Client Reputation	***GB - Plans:***					
		GB	Monthly	7,500 GB Plan	7,500	3,200.00
		GB	Monthly	15,000 GB Plan	15,000	3,600.00
		GB	Monthly	30,000 GB Plan	30,000	4,200.00
		GB	Monthly	45,000 GB Plan	45,000	4,800.00
		GB	Monthly	75,000 GB Plan	75,000	5,400.00
		GB	Monthly	105,000 GB Plan	105,000	6,000.00
		GB	Monthly	150,000 GB Plan	150,000	6,600.00
		GB	Monthly	300,000 GB Plan	300,000	9,000.00
	GB - Overage (prices are per GB):					
		GB	As Incurred	7,500 GB Plan		0.30

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	GB	As Incurred	15,000 GB Plan		0.28
	GB	As Incurred	30,000 GB Plan		0.26
	GB	As Incurred	45,000 GB Plan		0.24
	GB	As Incurred	75,000 GB Plan		0.21
	GB	As Incurred	105,000 GB Plan		0.18
	GB	As Incurred	150,000 GB Plan		0.15
	GB	As Incurred	300,000 GB Plan		0.12

DDoS Fee Protection

DDoS Protection ***Notes:***

DDoS Fee Protection requires WAF as a prerequisite (and can only be bought with WAF). It is a flat fee; there is no overage. It also has a Capped burst fee of $10,000 as incurred.

DDoS Protection	***Base Fee:***		**Plan**	**Incl. Amount**	
DDoS Protection	***GB - Plans:***				
	GB	Monthly	7,500 GB Plan	7,500	400.00
	GB	Monthly	15,000 GB Plan	15,000	800.00
	GB	Monthly	30,000 GB Plan	30,000	1,200.00
	GB	Monthly	45,000 GB Plan	45,000	1,600.00
	GB	Monthly	75,000 GB Plan	75,000	2,000.00
	GB	Monthly	105,000 GB Plan	105,000	2,400.00
	GB	Monthly	150,000 GB Plan	150,000	2,800.00
	GB	Monthly	300,000 GB Plan	300,000	3,200.00
DDoS Protection	***Additional Fees:***				
	Capped burst fee:				
		As Incurred			10,000.00

Compliance Management

Compliance Mgmt. ***Base Fee:***

PCI Compliance Management:

Monthly 400.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
Prolexic Routed						
Prolexic Routed	***Notes:***					
	A customer buys a primary Routed for a certain usage tier. Additional Routed can be purchased for a specific usage tier, and usage is aggregated and then overage is assessed at the combined usage tier. The largest Routed must be the primary Routed. Routed usage should be aggregated to one line on the order form. The aggregate Routed usage should have one overage rate on the order form.					
Prolexic Routed	***Included:***					
	Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	Monthly	1		
	Client Border Routers:					
		Routers	Monthly	2		
Prolexic Routed	***ALWAYS-ON - Base Fee:***			Plan	Incl. Amount	
Prolexic Routed	***ALWAYS-ON - Mbps clean inbound traffic - Primary Routed:***					
		Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	11,160.00
		Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	12,888.00
		Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	14,120.00
		Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	15,368.00
		Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	17,200.00
		Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	19,800.00
		Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	24,920.00
	ALWAYS-ON - Mbps clean inbound traffic - Additional Routed:					
		Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	8,928.00
		Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	10,312.00
		Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	11,296.00
		Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	12,296.00
		Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	13,760.00
		Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	15,840.00
		Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	19,936.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	ALWAYS-ON - Mbps clean inbound traffic - Overage (prices are per Mbps clean inbound traffic):					
		Mbps clean inbound traffic	As Incurred	50 Mbps Plan		56.00
		Mbps clean inbound traffic	As Incurred	100 Mbps Plan		40.00
		Mbps clean inbound traffic	As Incurred	200 Mbps Plan		35.20
		Mbps clean inbound traffic	As Incurred	300 Mbps Plan		32.00
		Mbps clean inbound traffic	As Incurred	500 Mbps Plan		28.00
		Mbps clean inbound traffic	As Incurred	700 Mbps Plan		24.00
		Mbps clean inbound traffic	As Incurred	1,000 Mbps Plan		20.00
Prolexic Routed	***ON-DEMAND - Base Fee:***			**Plan**	**Incl. Amount**	
Prolexic Routed	***ON-DEMAND - Mbps clean inbound traffic - Primary Routed:***					
		Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	6,560.00
		Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	7,568.00
		Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	8,288.00
		Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	9,016.00
		Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	9,832.00
		Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	11,312.00
		Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	14,608.00
	ON-DEMAND - Mbps clean inbound traffic - Additional Routed:					
		Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	5,248.00
		Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	6,056.00
		Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	6,632.00
		Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	7,216.00
		Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	7,872.00
		Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	9,056.00
		Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	11,328.00
	ON-DEMAND - Mbps clean inbound traffic - Overage (prices are per Mbps clean inbound traffic):					
		Mbps clean inbound traffic	As Incurred	50 Mbps Plan		84.00
		Mbps clean inbound traffic	As Incurred	100 Mbps Plan		60.00
		Mbps clean inbound traffic	As Incurred	200 Mbps Plan		52.80
		Mbps clean inbound traffic	As Incurred	300 Mbps Plan		48.00
		Mbps clean inbound traffic	As Incurred	500 Mbps Plan		42.00
		Mbps clean inbound traffic	As Incurred	700 Mbps Plan		36.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		Mbps clean inbound traffic	As Incurred	1,000 Mbps Plan		30.00
Prolexic Routed	***Additional Options:***					
	ALWAYS-ON - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	Monthly	1	999,999,999	1,680.00
	ON-DEMAND - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	Monthly	1	999,999,999	960.00
	Client Border Routers:					
		Routers	Monthly	1	999,999,999	800.00
	Disaster Recovery:					
		Locations	Monthly	1	999,999,999	2,560.00
	Flow-based Monitoring					
		Per Router	Monthly			960.00
	Application-based Monitoring					
		Per Appliance	Monthly			2,560.00
	Application-based Monitoring - SSL					
		Per Appliance	Monthly			4,480.00
Prolexic Routed	***Provisioning Fees:***					
Prolexic Routed	***ALWAYS-ON - Provisioning:***			Plan		
Prolexic Routed	***Provisioning - ALWAYS-ON - Mbps clean inbound traffic - Primary Routed:***					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		8,500.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		9,556.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		10,464.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		11,092.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		12,096.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		13,920.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		17,524.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Provisioning - ALWAYS-ON - Mbps clean inbound traffic - Additional Routed:					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		7,648.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		8,600.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		9,420.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		9,980.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		10,888.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		12,528.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		15,772.00
Prolexic Routed	***ON-DEMAND - Provisioning:***			**Plan**		
Prolexic Routed	***Provisioning - ON-DEMAND - Mbps clean inbound traffic - Primary Routed:***					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		8,500.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		9,556.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		10,464.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		11,092.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		12,096.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		13,920.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		17,524.00
	Provisioning - ON-DEMAND - Mbps clean inbound traffic - Additional Routed:					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		7,648.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		8,600.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		9,420.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		9,980.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		10,888.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		12,528.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		15,772.00
Prolexic Routed	***Provisiong - Additional Options:***					
	ALWAYS-ON - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	One Time			2,016.00
	ON-DEMAND - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	One Time			1,152.00
	Client Border Routers:					

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Routers	One Time			960.00
Disaster Recovery:					
	Locations	One Time			3,072.00
Flow-based Monitoring					
	Per Router	One Time			1,152.00
Application-based Monitoring					
	Per Appliance	One Time			3,072.00
Application-based Monitoring - SSL					
	Per Appliance	One Time			5,376.00

Prolexic Connect

Prolexic Connect	***Notes:***				

A customer buys a primary Connect for a certain usage tier. Additional Connect can be purchased for a specific usage tier, and usage is aggregated and then overage is assessed at the combined usage tier. The largest Connect must be the primary Connect. Connect usage should be aggregated to one line on the order form. The aggregate Connect usage should have one overage rate on the order form.

Prolexic Connect	***Included:***				
	Subnets (Per block of 8 x /24 subnets):				
	Subnet Block	Monthly	1		
	Prolexic Connect				
	Location	Monthly	1		

Prolexic Connect	***ALWAYS-ON - Base Fee:***		Plan	Incl. Amount	
Prolexic Connect	***ALWAYS-ON - Mbps clean inbound traffic - Connect:***				
	Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	18,936.00
	Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	19,664.00
	Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	21,120.00
	Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	22,576.00
	Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	25,488.00
	Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	28,400.00
	Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	32,768.00

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		Mbps clean inbound traffic	Monthly	2,000 Mbps Plan	2,000	45,936.00
	ALWAYS-ON - Mbps clean inbound traffic - Overage (prices are per Mbps clean inbound traffic):					
		Mbps clean inbound traffic	As Incurred	50 Mbps Plan		72.80
		Mbps clean inbound traffic	As Incurred	100 Mbps Plan		52.00
		Mbps clean inbound traffic	As Incurred	200 Mbps Plan		45.76
		Mbps clean inbound traffic	As Incurred	300 Mbps Plan		41.60
		Mbps clean inbound traffic	As Incurred	500 Mbps Plan		36.40
		Mbps clean inbound traffic	As Incurred	700 Mbps Plan		31.20
		Mbps clean inbound traffic	As Incurred	1,000 Mbps Plan		26.00
		Mbps clean inbound traffic	As Incurred	2,000 Mbps Plan		20.80
Prolexic Connect	***ON-DEMAND - Base Fee:***			**Plan**	**Incl. Amount**	
Prolexic Connect	***ON-DEMAND - Mbps clean inbound traffic - Connect:***					
		Mbps clean inbound traffic	Monthly	50 Mbps Plan	50	10,820.00
		Mbps clean inbound traffic	Monthly	100 Mbps Plan	100	11,236.00
		Mbps clean inbound traffic	Monthly	200 Mbps Plan	200	12,068.00
		Mbps clean inbound traffic	Monthly	300 Mbps Plan	300	12,900.00
		Mbps clean inbound traffic	Monthly	500 Mbps Plan	500	14,564.00
		Mbps clean inbound traffic	Monthly	700 Mbps Plan	700	16,228.00
		Mbps clean inbound traffic	Monthly	1,000 Mbps Plan	1,000	18,724.00
		Mbps clean inbound traffic	Monthly	2,000 Mbps Plan	2,000	26,248.00
	ON-DEMAND - Mbps clean inbound traffic - Overage (prices are per Mbps clean inbound traffic):					
		Mbps clean inbound traffic	As Incurred	50 Mbps Plan		72.80
		Mbps clean inbound traffic	As Incurred	100 Mbps Plan		52.00
		Mbps clean inbound traffic	As Incurred	200 Mbps Plan		45.76
		Mbps clean inbound traffic	As Incurred	300 Mbps Plan		41.60
		Mbps clean inbound traffic	As Incurred	500 Mbps Plan		36.40
		Mbps clean inbound traffic	As Incurred	700 Mbps Plan		31.20
		Mbps clean inbound traffic	As Incurred	1,000 Mbps Plan		26.00
		Mbps clean inbound traffic	As Incurred	2,000 Mbps Plan		20.80
Prolexic Connect	***Additional Options:***					
	ALWAYS-ON - Subnets (Per block of 8 x /24 subnets):					

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		Subnet Block	Monthly	1	999,999,999	1,680.00
	ON-DEMAND - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	Monthly	1	999,999,999	960.00
	Flow-based Monitoring					
		Per Router	Monthly			960.00
	Application-based Monitoring					
		Per Appliance	Monthly			2,560.00
	Application-based Monitoring - SSL					
		Per Appliance	Monthly			4,480.00
Prolexic Connect	***Provisioning Fees:***					
Prolexic Connect	***ALWAYS-ON - Provisioning:***			**Plan**		
Prolexic Connect	***Provisioning - ALWAYS-ON - Mbps clean inbound traffic -Connect:***					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		12,984.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		13,484.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		14,484.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		15,480.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		17,476.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		19,476.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		22,468.00
		Mbps clean inbound traffic	One Time	2,000 Mbps Plan		31,500.00
Prolexic Connect	***ON-DEMAND - Provisioning:***			**Plan**		
Prolexic Connect	***Provisioning - ON-DEMAND - Mbps clean inbound traffic - Connect:***					
		Mbps clean inbound traffic	One Time	50 Mbps Plan		12,984.00
		Mbps clean inbound traffic	One Time	100 Mbps Plan		13,484.00
		Mbps clean inbound traffic	One Time	200 Mbps Plan		14,484.00
		Mbps clean inbound traffic	One Time	300 Mbps Plan		15,480.00
		Mbps clean inbound traffic	One Time	500 Mbps Plan		17,476.00
		Mbps clean inbound traffic	One Time	700 Mbps Plan		19,476.00
		Mbps clean inbound traffic	One Time	1,000 Mbps Plan		22,468.00
		Mbps clean inbound traffic	One Time	2,000 Mbps Plan		31,500.00
Prolexic Connect	***ON-DEMAND - Additional Locations:***					
	Provisioning - Additional Locations:					

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
		Additional Location	One Time	1	999,999,999	8,000.00
Prolexic Connect	***Provisiong - Additional Options:***					
	ALWAYS-ON - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	One Time			2,016.00
	ON-DEMAND - Subnets (Per block of 8 x /24 subnets):					
		Subnet Block	One Time			1,152.00
	Flow-based Monitoring					
		Per Router	One Time			1,152.00
	Application-based Monitoring					
		Per Appliance	One Time			3,072.00
	Application-based Monitoring - SSL					
		Per Appliance	One Time			5,376.00
Enhanced Support SLA						
ESLA	***Notes:***					
	Fixed MRR when sold as an add-on to Standard Support. Enhanced Support SLA and unlimited number of support cases are included with the base fee. Under the % Fee Model, the base fee equals 5% of the total committed value (using wholesale rates) for non-services products, including and committed delivery charges (minimum of $200). This is calculated at time of deal and entered as a fixed-MRR item. This fee will be adjusted at renewal by applying the same calculation to the new committed value.					
ESLA	***Base Fee:***					
	Enhanched Support SLA - Sold on Standard Support (% price model; i.e. % of total committed value for non-services products):					
			Monthly			5.00%
Integration						
Integration	***Notes:***					

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
	Fixed MRR billed One Time/Monthly. Integration fees are charged per specific product integration. Emergency integration fees are charged in addition to the Standard or Managed integration fee. The number of hours (LOE) do not appear on the order form. If a specific number of hours needs to be called out, then the rep will use the SOW option and attached it to a PS Enterprise deal.					
Integration	***Web Experience - Consumer:***					
Web Exp. Consumer	***Ion Standard - Standard Integration***		One Time			9,000
	Ion Standard - Managed Integration		One Time			20,000
	Dynamic Site Accelerator - Standard Integration		One Time			5,000
	Dynamic Site Accelerator - Managed Integration		One Time			18,000
	Emergency Standard		One Time			10,000
	Emergency Managed		One Time			20,000
Integration	***Media:***					
Media	***Adaptive Media Delivery - Standard***		One Time			3,000
	Dynamic Site Delivery - Standard		One Time			3,500
	Dynamic Site Delivery - Managed		One Time			9,500
	Content Targeting - Standard		One Time			1,200
	Content Targeting - Managed		One Time			6,000
	Site Failover - Standard		One Time			2,000
	Site Failover - Managed		One Time			6,000
	Dynamic Content Assembly		One Time			1,000
	Client Side Access Control - Standard		One Time			2,000
	Client Side Access Control - Managed		One Time			3,000
	Media Services - Live - Standard		One Time			3,000
	Media Services - On Demand - Standard		One Time			3,000
Integration	***Security:***					
	Kona Site Defender - Standard		One Time			20,000
Security	***Fast DNS - Standard***		One Time			5,000
	Fast DNS - Managed		One Time			14,000
Named Enhanced Support						

AT&T Content Delivery Network Service IaaS

	Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
NES	***Base Fee:***					
	Named Enhanced Support					
			Monthly			5,000.00
PS Enterprise						
PS Enterprise	***Notes:***					
	Sales have details specified in a Statement of Work ("SOW").					
PS Enterprise	***Base Fee:***					
	PS Hours (One time & Monthly):					
		Hours	As Incurred	0	999,999,999	300.00
Service Management Package 2.0						
SMP	***Notes:***					
	The customer can choose from two different packages: Service Management or Rule Update Service.					
Service Mgmt. Pkg.	***Base Fee:***					
	Service Management:					
			Monthly			3,000.00
Service Mgmt. Pkg.	***Included:***					
	Configurations under Optimization Schedule:					
		Configurations	Monthly	2		
	PS Hours:					
		Hours	Monthly	18		
Rule Update Srv.	***Base Fee:***					
	Rule Update Service:					
			Monthly			4,500.00
Rule Update Srv.	***Included:***					
	Threat Update Reviews:					
		Reviews	Monthly	3		

AT&T Content Delivery Network Service IaaS

Item Name	UOM	Billing Frequency	Tier Start	Tier End	State Contract Retail
PS Security Specialist Hours:					
	Hours	Monthly	24		

Attachment E Contractor's Response to the Solicitation

AT&T Response to State of Utah's Solicitation # CH16012 for Cloud Services

4393 Riverboat Road
4th Floor
Taylorsville, UT 84123
www.att.com

Office: 801-556-3236
Fax: 801-313-8315
sf7074@att.com

March 10, 2016

Christopher Hughes
Contracts Analyst
DAS
801-538-3254
christopherhughes@utah.gov

RE: Solicitation CH16012 – NASPO ValuePoint Cloud Solutions

Dear Mr. Hughes:

AT&T is pleased to present our cloud-based solution to the lead State of Utah Division of Purchasing, as well as other participating entities, in conjunction with the NASPO ValuePoint Cooperative Purchasing Program. We understand your requirements and present a proposal we believe uniquely positions AT&T to meet the NASPO service and product needs outlined in the RFP.

Based on the instructions in Section 5.2 of the RFP, we include required statements below.

- (5.2.1) AT&T understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.
- (5.2.2) AT&T created a task force consisting of more than 30 individuals in the preparation of this response. The team consisted of both internal and external best-in-class resources. Key contribution areas included
  - Cloud Computing Specialists
  - Network Architecture and Infrastructure engineers
  - Government sales and marketing leadership
  - Consortium and Association management team
  - Finance
  - Legal
  - Contract Management
  - Product Management
  - Technical and Applications Solutions Support
- (5.2.3) AT&T is not listed on a government debarment list. We're unaware of a disqualification or debarment that would negatively affect our ability to provide your products and services. This means that we're committed to fully complying with state and federal regulations.

- (5.2.4) AT&T acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any other Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.
- (5.2.5) AT&T is proposing a broad array of service and deployment model(s) under the terms of the RFP including: SaaS, IaaS, and PaaS.
- (5.2.6) AT&T understands the concerns that virtually all of our customers have regarding the care of data that may reside in or be operated upon within our various services. We handle all data entrusted to us by customers carefully and thoughtfully. Using FIP Publication 199 as a guide, we have reviewed the particular services offered in this proposal and have determined that the most appropriate category of data risk would be "Low Risk Data."

AT&T Proposed Product	Risk Category
AT&T Conferencing with Cisco WebEx	SaaS
AT&T Video Meetings with Blue Jeans	SaaS
AT&T Cloud Web Security Service	IaaS
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS
AT&T Unified Communications as a Service	SaaS
AT&T Hosted Contact Center Service	SaaS
AT&T Premises-Based Firewall Service	IaaS
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS
AT&T Professional Services	IaaS
AT&T Content Delivery Network Service	IaaS

The AT&T solution is flexible enough to meet your changing operational needs while satisfying your requirements. It also allows for the participating entities to scale the solution based on the challenges they face in today's ever changing technology market.

AT&T has a very successful relationship with NASPO ValuePoint and we look we look forward to working with State of Utah and other participating entities on this important initiative. I'll follow up with you soon to discuss our proposed solution.

Sincerely,

Shannon Archer

Shannon Archer
Client Solutions Executive

AT&T Response to State of Utah's Bid # CH16012 for Cloud Services

March 10, 2016

Shannon Archer
Client Solutions Executive
AT&T
4393 Riverboat Rd
Taylorsville, UT 84123
Office: 801-556-3236
Email: sf7074@att.com

Proposal Validity Period—The information and pricing contained in this proposal is valid for a period of one hundred eighty (180) days from the date written on the proposal cover page or until the E-rate filing window closes for the upcoming E-rate Funding year, whichever occurs later, unless rescinded or extended in writing by AT&T Corp.
Terms and Conditions—This proposal is conditioned upon negotiation and execution by the parties of a written agreement containing mutually acceptable terms and conditions.
Proposal Pricing—Pricing proposed herein is based upon the specific product/service mix and locations outlined in this proposal, and is subject to the standard terms and conditions for those products and services and the AT&T E-rate Rider unless otherwise stated herein. Any changes or variations in AT&T Corp.'s standard terms and conditions the products/services, length of term, locations, and/or design described herein may result in different pricing.
Providers of Service—Subsidiaries and affiliates of AT&T Inc. provide products and services under the AT&T brand. Where required, an AT&T Affiliate authorized by the appropriate regulatory authority will be the service provider. AT&T Corp. is the bidding entity and will be the entity financially responsible for performance of the agreement.
Broadband Internet Access—For information about AT&T's broadband Internet access services, please visit www.att.com/broadbandinfo.
End User Equipment—Beginning with funding year 2015, E-rate recipients must cost allocate non-ancillary ineligible components that are bundled with eligible products or services, including those end user device components that previously would have fallen within the scope of components not requiring cost allocation as described in the 2010 Clarification Order. Cost allocations are the responsibility of E-rate Applicants. When AT&T provides an AT&T Mobility voice and data bundled plan, applicants can use 49% for voice and 51% for data in their cost allocations. For additional information, reference USAC /SLD website @ http://www.usac.org/sl/ and Cost Allocation Guidelines for Services @ http://www.usac.org/sl/applicants/beforeyoubegin/eligible-services/cost-allocations.aspx. Equipment availability and pricing is subject to change based on when plans are activated.
Disclaimer—For purposes of this Proposal, the identification of certain services as "eligible" or "non-eligible" for Universal Service ("E-rate") funding is not dispositive, nor does it suggest that this or any other services in this Proposal will be deemed eligible for such funding. Any conclusions regarding the eligibility of services for E-Rate funding must be based on several factors, many of which have yet to be determined relative to the proposed services and equipment described herein. Such factors will include, without limitation, the ultimate design configuration of the network, the specific products and services provisioned to operate the network, and the type of customer, and whether the services are used for eligible educational purposes at eligible locations. In its proposal, AT&T will take guidance from the "Eligible Services List" and the specific sections on product and service eligibility on the Schools and Libraries Division ("SLD") of the Universal Service Administrative Company ("USAC") website www.usac.org/sl. This site provides a current listing of eligible products and services, as well as conditionally eligible and ineligible services. This guidance notwithstanding, the final determination of eligibility will be made by the SLD after a review of the customer's E-rate application for this proposal. If AT&T is awarded the bid for this project, AT&T will provide assistance on the E-Rate application solely on matters relative to the functionality of the services and products which comprise the network. Nevertheless, the responsibility for the E-rate application is with the customer. AT&T is not responsible for the outcome of the SLDs decision on these matters.

Table of Contents

AT&T Attachments

A Signed Acknowledgement of Amendment

B Completed Consensus Assessment Initiative Questionnaires (CAIQs)

C AT&T Service Guides with Service Level Agreements

D AT&T Business Continuity Handbook

E AT&T Information & Network Security Customer Reference Guide

F AT&T Data Security Addendum

G AT&T Additional Cloud Services

1. RFP Signature Page

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.

5.1 (M) SIGNATURE PAGE

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an **ORIGINAL HANDWRITTEN** signature executed in **INK** OR **AN ELECTRONIC SIGNATURE**, and be returned with the Offeror's proposal.

AT&T Response:

AT&T understands, and complies. We completed the vendor information form, with electronic signature, via the Bidsync system.

2. Executive Summary

5.4 (M) EXECUTIVE SUMMARY

AT&T Response:

To provide quality public service, government agencies must improve efficiencies, upgrade to the latest technologies, and find ways to satisfy the changing needs of their constituents. Therefore, government agencies like the State of Utah, are looking at new ways to realign old practices with evolving technologies.

Based on your current organizational requirements, you have recognized the need for optimizing your hosted cloud environment to improve the overall end user responsiveness and satisfaction. To achieve this, you want to understand industry best practices and deliver a scalable solution. Therefore, you are looking for a qualified hosting vendor to provide comprehensive, cost-effective, and secured cloud services that helps to meet your current and future objectives.

AT&T can help you strengthen and extend your use of emerging cloud-based services and provide the expertise to move your operations to the next generation of technology in a cost-effective manner. We offer a range of reliable, high-quality, and stable cloud services.

The State of Utah must have an infrastructure in place that will support operations and future objectives effectively. We can help you redefine your value in the government sector by building a network platform to support these objectives:

- Increase the productivity and efficiency of your staff
- Improve your operational efficiency
- Consolidate vendors

Solution

AT&T is pleased to propose a range of cloud-based and related services as outlined in the table below. We describe these offerings more fully throughout our proposal.

AT&T Conferencing with Cisco WebEx	SaaS
Part of Cisco's collaboration portfolio delivered by AT&T, AT&T Conferencing with Cisco WebEx allows you to hold interactive meetings, conduct engaging events, deliver live sales presentations, and implement remote learning programs – all with 24-hour customer support. AT&T provides on-demand, integrated web/audio/video conferencing and remote collaboration capabilities featuring Cisco WebEx. Delivered as a cloud based service and supported by a world class sales and technical support team, we can provide a superior set of solutions tailored specifically for every area of your business. Our Collaboration Meeting	

Room add-on combines the simplicity of WebEx conferencing with an always-available video bridging capability for hosts to provide a common meeting experience for standards-based video systems, web participants or mobile devices.	
AT&T Video Meetings with Blue Jeans	**SaaS**
AT&T Video Meeting with Blue Jeans is a global videoconferencing service that makes face-to-face collaboration accessible, high quality, and cost-effective for all businesses, regardless of size. We use the cloud to connect traditionally incompatible video services and devices together, enabling you to easily host multi-party video meetings from a desktop, mobile device, or conference room video system. To further enable productive collaboration, AT&T Video Meeting with Blue Jeans lets you share presentations, documents, and even video files in real-time during your video meetings.	
AT&T Cloud Web Security Service	**SaaS**
AT&T Cloud Web Security Service (Cloud WSS) is designed to provide comprehensive Web security including real-time protection against viruses and malware, protection against compromised/hacked web sites and granular control of Web applications.	
AT&T Distributed Denial of Service (DDoS) Defense Service	**IaaS**
AT&T Distributed Denial of Service (DDoS) Defense Services provides DDoS attack identification and mitigation within the AT&T backbone providing increased protection from malicious traffic before it reaches a customer's network.	
AT&T Unified Communications as a Service	**SaaS**
Part of Cisco's collaboration portfolio delivered by AT&T, AT&T Unified Communications (UC) Services is a secure cloud-based communication and collaboration service. AT&T UC Services provides business-class IP Voice Telephony and can enable an integrated set of communication capabilities for Instant Messaging and Presence, Video Telephony, Voicemail and Integrated Messaging, all from an IP phone, mobile phone, or desktop client. This UC service also integrates seamlessly with Cisco WebEx conferencing to ultimately provide a complete unified and simplified end user experience.	
AT&T Hosted Contact Center Service	**SaaS**
AT&T Hosted Contact Center Service (AT&T Partner, inContact) helps call centers around the globe create profitable customer experiences through its powerful portfolio of cloud-based call center call routing, self-service, and agent optimization solutions. The inContact services and solutions enable call centers to operate more efficiently, optimize the cost and quality of every customer interaction, and helps ensure ongoing customer-centric business improvement and growth.	
AT&T Premises-Based Firewall Service	**IaaS**
AT&T Premises-Based Firewall Service provides firewall/unified threat management protection at the perimeter of the customer's premises, and enforcement of location specific security policies. Configurations include Juniper, Fortinet, Palo Alto, Checkpoint, and Cisco.	
AT&T Managed Intrusion Detection/Intrusion Prevention Service	**IaaS**
AT&T Managed Intrusion Detection/Intrusion Prevention Service is a fully managed, comprehensive, IP network attack recognition and response solution for network security. There is a premises-based hardware/software solution option with AT&T providing the hardware/ software components and continuous support through the AT&T Security Network Operations Center.	
AT&T Professional Services	**IaaS**
AT&T can provide a range of professional services including consulting and training services. We can assist with developing security policies, storage management policies, migration planning, disaster recovery planning, and virtualization/rightsizing.	
AT&T Content Delivery Network Service	**IaaS**
AT&T offers our AT&T Content Delivery Network Service via Akamai, the global leader in Content Delivery	

Network (CDN) services, making the Internet fast, reliable, and secure for its customers. Akamai has deployed the most pervasive, highly distributed CDN with more than 200,000 servers in more than 110 countries and within more than 1,400 networks around the world. The CDN solution provides significant value for any hosted applications that use the Public Internet for delivery to end users. This provides benefits such as higher availability, more consistent content delivery, faster end user experience, and optimal sizing of cloud service resources. The Akamai CDN solutions that we propose can be grouped into three main product portfolios: Media Delivery, Web Acceleration, and Web Security, and are all delivered as Managed Services.

AT&T has both rich experience and proven success in integrating and managing networks and network infrastructure for organizations like yours.

Personalized Support

We understand the importance of personalized service, we give you an account team of specialists to design and implement your new solution. You'll receive ongoing, coordinated support from your account team for all of your AT&T services.

State of Utah's AT&T Account Team

Name	Title	Phone Number	Email
Shannon Archer	Client Solutions Executive	801-556-3236	sf7074@att.com
Rick Frankhuizen	Senior Customer Contract Manager	661-263-9835	wf2146@att.com
Bethani Cross	Client Solutions Executive – GPO – NASPO	214-679-9053	bc4732@att.com
Leadership Team			
Gary Tingey	Sales Manager – State of Utah	801-493-9190	gt0233@att.com
Andy Meissner	Director – Solutions Architecture	908-234-3492	am1282@att.com
Paula Brunson	Sales Director – GPO – NASPO	940-368-5700	pd4719@att.com

3. Mandatory Minimums

This section should constitute the Offeror's point-by- point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

AT&T Response:

AT&T has read, understands, and complies. Please see the following point-by-point responses to the applicable Section 5 requirements of the RFP.

5 MANDATORY MINIMUM REQUIREMENTS

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each mandatory minimum requirement. If a mandatory minimum requirement is not applicable to an Offeror's Solution then the Offeror must explain why the mandatory minimum 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.

AT&T Response:

AT&T has read, understands and complies. Please see the following point-by-point response to each mandatory minimum requirement.

5.2 (M) COVER LETTER

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.

5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

AT&T Response:

AT&T understands and complies. Please refer to our cover letter at the beginning of our response for all of the required components.

5.3 (M) ACKNOWLEDGEMENT OF AMENDMENTS

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

AT&T Response:

AT&T understands and complies. AT&T includes our signed Acknowledge of Amendment in Attachment A of our response.

5.5 (M) GENERAL REQUIREMENTS FOR THE SERVICE OFFERINGS

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.

AT&T Response:

AT&T has a dedicated reporting team which will prepare and provide the quarterly reporting to NASPO. The reporting team manager will compile and send reports quarterly per the requirements outlined.

AT&T intends to address this requirement in a manner similar to that which is already in place for the AT&T wireless services currently available to NASPO members. In brief, AT&T intends to review as-billed charges incurred by NASPO members who will have procured services under this contract and tally up said charges to calculate an administrative fee. AT&T personnel will then remit payments as appropriate. AT&T intends to perform this work on a quarterly rather than a monthly basis. AT&T reserves the right to modify the format of any reports generated with approval from NASPO as to form and content.

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.

AT&T Response:

AT&T has read and understands.

AT&T agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading AT&T ordering instructions if awarded a contract.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment[1]. Offeror must either submit a completed The

[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.

Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

AT&T Response:

AT&T understands and complies. Please refer to our completed CAIQs for applicable products in Attachment B.

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.

AT&T Response:

AT&T understands and complies. Please refer to Attachment C for applicable Service Guides which include our Service Level Agreements (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.

AT&T Response:

AT&T agrees to certify with the State of Utah annually on attainment of technical capability standards awarded in the master agreement under this RFP.

[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.

4. Business Profile

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by- point response, in the order listed, to each requirement in the Section 6 of the RFP.

AT&T Response:

AT&T has read, understands, and complies. Please see the following point-by-point responses to Section 6 of the RFP.

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.**

Year Founded

The AT&T Corp. date of incorporation was March 3, 1885.

Organizational Structure

AT&T Corp. is a subsidiary of AT&T Inc.

AT&T Inc. is a publicly traded corporation.

We are an independent, publicly traded telecommunications services provider that has its headquarters in Dallas, Texas. No single person owns more than 10% of the company.

We're a global communication leader that offers you new services, products, and solutions.

Client Base

AT&T serves millions of customers around the world, including global, national, mid-size, regional, and government customers. Currently we provide service for all of the Fortune 1000 companies.

We are proud to provide our customers with a strong product and service line, thanks to our focus on delivering the industry's most reliable service, most globally consistent portfolio, and the most advanced network management and security tools.

AT&T has a vertical focus on the Government segment including dedicated sales, marketing and technical professionals bringing best in class government solutions to customers in the segment. Customers range from large state governments to small municipalities.

AT&T Growth

AT&T recorded consolidated revenues ($B) of $127.4 in 2012, $128.8 in 2013, $132.4 in 2014 and $146.8 in 2015 allowing AT&T to recognize 15% consolidated revenue growth for this time period.

Employee Information

Number of Employees

AT&T has 280,000 employees.

Employee Retention Rate

AT&T enjoys a better than industry average retention rate, even with the competitive demands for resources in the telecommunications industry. The AT&T annualized turnover rate for the past two years is as follows:

- 2014 10.2%
- 2013 10.2%

It should be noted that AT&T has decreased our retention rate percentage year after year for the past eight years.

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 services identical or very similar to those required by this RFP. Government experience is preferred.

AT&T Response:

AT&T is viewed as an industry leading integrated solutions provider in the Government Sector. Offering a wide array of products and services specifically tailored to meet the ever demanding and changing needs of government agencies.

AT&T has a dedicated team of sales professionals, product managers, and industry solutions specialists which focus on solving the needs of our clients in the government space generating in excess of $5 billion in revenues annually.

Over the past 15+ years, AT&T has developed a robust portfolio of consortium agreements and contracting practices. AT&T uses the master agreement strategy with participating addendums in dealing with all its key consortium partners, including NASPO today. This contracting methodology gives the participating agency the flexibility to purchase the products and services desired at the local level with ease in contracting.

AT&T has a strong commitment to the government vertical via our external affairs partnerships, local market initiatives, and participation in industry events which benefit government agencies as they navigate the technology challenges they face today and in the future.

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.

AT&T Response:

Financial Statements

Please refer to the below link for AT&T's audited financial statements:
http://www.att.com/gen/investor-relations?pid=9186

D&B Rating

In its recent Business Information Report, Dun and Bradstreet (D&B) rates AT&T positively.

Our current D&B rating is 5A2. For additional financial information, you can visit our Investor Relations website at http://www.att.com/gen/landing-pages?pid=5718. In addition, because we're a publicly held company, most key information about AT&T can be acquired from rating and reporting agencies.

When you consider our D&B rating and other financial data, you can see we're a stable company that's experiencing expanding margins and increasing revenue growth.

Credit Rating

AT&T has high credit ratings with four major agencies. These ratings include the following:

- Dun & Bradstreet (D&B): 5A2 (2015)
- Fitch: A- (2015)
- Moody's: Baa1 (2015)
- Standard & Poor's (S&P): BBB+ (2015)

In addition, AT&T's 2015 Fortune 500 rankings are 12 (U.S.) and 34 (global).

So, our high credit ratings reflect our sound financial health.

DUNS Number

The AT&T Corp. Data Universal Numbering System (D-U-N-S®) number is 00-698-0080.

6.4 (E) GENERAL INFORMATION

6.4.1 Provide any pertinent general information about the depth and breadth of your services and their overall use and acceptance in the cloud marketplace.

AT&T Response:

For more than a century, AT&T has consistently provided innovative, reliable, high-quality products and services and excellent customer care. We invest in world-class people, processes, tools, and training and follow high security standards to help protect customers from the risks and challenges that confront businesses today.

Today, our mission is to connect people with their world, everywhere they live and work, and do it better than anyone else. We're fulfilling this vision by creating new solutions for consumers, businesses, and government agencies, and by driving innovation in the communications and entertainment industry.

We have extensive experience with a wide portfolio of communication products and services, and we're experts at designing solutions to match the needs of NASPO and its participants. NASPO will receive ongoing, coordinated support from AT&T for all of its AT&T services.

Our proposal confirms that we understand your objectives and have the expertise and resources to support them. We look forward to working with NASPO to implement cloud and application solutions and help each State adopt their information technology strategy.

AT&T is a global leader in communications and a recognized leader in business-related voice and data services, including global IP services, hosting, applications, and managed services. Businesses all over the world deploy AT&T services to improve productivity, manage overall costs, and position themselves to take advantage of future technology enhancements.

The services being proposed by AT&T are intended to help NASPO extend and optimize its existing IT operations. Our response is illustrative of our resolve to deploy innovative and stable technologies to drive economic efficiencies for NASPO and its participants. AT&T is committed to working with NASPO and its partners to provide a range of high-quality cloud-based services.

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.

AT&T Response:

As of June 15, 2011, AT&T has adopted the new Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). SSAE 16/ISAE 3402 replaced the Statement on Auditing Standards No. 70 (SAS 70) standard as the professional standard for service organizations to obtain an independent assessment about the effectiveness of internal controls that are relevant to their customer's financial statements. SSAE 16/ISAE 3402 is based heavily on the preceding SAS 70 audit standard.

New services generally have to be in production (General Availability) for at least six months to be audited under a SOC 1 audit.

6.5 (E) BILLING AND PRICING PRACTICES

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

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

AT&T Response:

Our Cloud Services dashboard-style portal provides our customers with user management tools and capabilities useful for managing services such as the authorization of user's access, resource usage, performance management, and billing details, among others.

With the new cloud portal user management dashboard, our customers will be able to manage their users and gleam key insight into usage patterns and trends by company, group, or individual.

In addition, customers will have the ability to correlate and aggregate usage data with billing information.

Given the wide scope of products and services offered under this RFP, AT&T will work with participating entities to establish the billing platform that best meets their needs.

AT&T offers a variety of billing platform options to meet the needs of our clients based on product and customer payment choice.

AT&T has a seasoned team of service management executives that will assist participating entities in navigating the AT&T associated billing process and platform for the cloud-based service offering they select.

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

AT&T Response:

The AT&T cloud-based services offerings are truly scalable based on the needs of the Purchasing Entity.

Some of the products and services submitted under this solicitation have different potential costs that may need to be considered based on the environment of the participating entity and solution they are implementing.

AT&T will work closely with the participating entity to determine any potential cost impact prior to the implementation of any of the AT&T cloud-based solutions proposed herein. A few potential cost impacts have been noted as a reference to possible impediments.

- AT&T is proposing a hosted, managed solution, and therefore there are no implementation costs. The service is billed on a monthly basis for the audio usage and web conferencing licenses.
- The overages would apply to bursting capabilities on the purchased virtual ports service. Overages would also apply to overages on the event services of PrimeTime.
- If a Purchasing Entity wants to integrate AT&T Cloud Web Security with their Active Director there could be minimal cost to hosting the integration software on a member server of the domain.
- The contracted price of the service, times the service term is the total cost of the service.
- Cost impacts for the UC Voice service are primarily driven on a monthly basis by the subscribed users in a Price Times Quantity model. Additional ancillary services can also be added depending on the customer requirements that include the number of Auto Attendants, Attendant Consoles, Federation with

other IM systems, Advanced 911, legacy PBX integration, Group Announcements, Collaboration Edge requirements, and connectivity and PSTN access requirements. One-time effects can also impact cost due to equipment requirements for phones, routers, and voice gateways where needed.

- Typical sizing components for AT&T Premises-Based Firewall service are the amount of traffic flowing through the premise device, number of ports (DMZ, Extranet, etc.), equipment brand selection, High Availability or Single Availability, and the addition of any options for additional security functionality like web filtering, anti-virus, IPS, etc.
- Typical sizing components for AT&T Intrusion Detection/Prevention service are the amount of traffic flowing through the premise device, number of ports, equipment brand selection, High Availability or Single Availability, and the addition of any options.

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.

AT&T Response:

All of our services are compliant with NIST standards due to our extensive security engagements with Federal Agencies, State Agencies across the United States, and large enterprise customers with strict requirements for NIST compliance.

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.

AT&T Response:

The AT&T cloud-based service offerings include Infrastructure, Platform, and Software. As the technology landscape is constantly changing, AT&T has submitted service models which we believe agencies have an immediate need for and meet future requirements as well.

Please see the table below of service offerings submitted for your consideration in the response.

Service Being Proposed	Customer Category
AT&T Conferencing with Cisco WebEx	SaaS
AT&T Video Meetings with Blue Jeans	SaaS
AT&T Threat Manager	IaaS
AT&T Cloud Web Security Service	SaaS
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS
AT&T Unified Communications as a Service	IaaS
AT&T Hosted Contact Center Service	SaaS
AT&T Synaptic Storage as a Service	IaaS
AT&T Premises-Based Firewall Service	IaaS
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS
AT&T Professional Services	IaaS
AT&T Content Delivery Network Service	IaaS

6.7 (E) BEST PRACTICES

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.

AT&T Response:

For more than 136 years, AT&T has consistently provided innovative, reliable, high-quality products and services and excellent customer care. We invest in world-class people, processes, tools, and training and follow high security standards to help protect customers from the risks and challenges that confront businesses today.

With one of the largest global IP networks and 38 data centers around the world, AT&T has extensive network security knowledge, which is applied to protect our hosting facilities and thwart real-world threats.

AT&T has the ability today to integrate your applications into the cloud, mobilize them, and make them seamless. Our strategy is to deliver fully managed and integrated solutions by capitalizing on our mobility network, security strength, and leveraging our expertise to create integrated solutions. We'll work with PwC and its participants to support their needs and drive efficiency.

Managed Security

AT&T offers unmatched security expertise to help shield clients from the risks and complexities of managing a secure hosted infrastructure. Our layered security model provides multi-level protection across all information, data and physical assets. This model protects AT&T customers from both physical and logical security threats and employs a reinforced system of countermeasures so a single point of failure does not compromise the entire system.

The AT&T global security organization is comprised of over 800 certified and credentialed security professionals dedicated to the protection of the AT&T global network and its service offerings. Regardless of the services a customer contracts for, AT&T provides:

- Participation in Key Security Organizations (i.e. CERT, FIRST, NSTAS)
- Physical and Logical Access Controls
- Network Intrusion Detection
- Security Incident Reporting and Management
- Standards Compliance and Regulation (SSAE 16, PCI DSS, ISO27001)
- Stringent internal BCDR Planning
- Personnel Security Control Policies
- Ongoing Training and Certification

Physical Security

AT&T restricts and monitors physical access to its Internet Data Centers (IDCs) via numerous security measures. On-site security officers monitor IDC access. We further control access via thorough ingress and egress sign-in procedures, managed key and access card plans, hand bioscanners and mantraps, various managed access permissions and access request methods, and controlled access and egress doors. In addition, we use closed-circuit TV (CCTV) cameras to monitor access, egress, and IDC infrastructure.

We restrict non-employee IDC access to areas such as the lobby, customer lounge, conference rooms, common areas, and space that we allocate to customers. Additionally, we reserve the right to further restrict access to any part of the IDC at any time for safety and security reasons. This means that we work hard to secure our IDCs and allow only individuals with clearance to enter our facilities.

Access Policies

We use industry-standard access policies to help us protect AT&T facilities. Our site security program requires all employees, contractors, visitors, and guests to present an electronic access badge and photo ID. These badges are programmed to only enable access to approved areas.

To provide additional site security, we

- Escort visitors in our facilities
- Limit data center access to employees that require it to do their jobs
- Restrict access to our server racks to individuals with proper authorization
- Provide authorization from only the general manager or security group
- Routinely review our access records to make sure they're up to date and accurate

Encryption & Logging

For particularly sensitive applications (e.g. those which store and process Personal Healthcare Information), we recommend that customers incorporate additional hardware and/or software based encryption into the infrastructure design. We further recommend that customer technical staff maintain responsibility for retaining and managing encryption keys. In addition, we recommend the incorporation of access logging (e.g. outboard logging appliances) into the security fabric. These appliances provide a record of access attempts into sensitive components within the infrastructure and are a valuable aid in conducting forensics.

Service Management Philosophy

As a global communications carrier with over 100 years of experience, AT&T has developed its own approaches to the functions described in the ITIL framework. The AT&T approaches could be described as ITIL-compliant, since all functions are addressed, although our practices may be somewhat different than those specified by ITIL. AT&T has had an ITIL maturity assessment performed using third parties for selected managed services.

AT&T has seen the most applicability of the ITIL best practices in the area of Service Management, which is part of the AT&T Worldwide Customer Care organization. Our approach to utilizing the ITIL Service Management best practices has been to apply

them to two specific areas of the relationship between a Customer's IT service management and the AT&T service management environments:

1. At the customer interface
2. Within AT&T Service Management centers

Though AT&T has standard approaches regarding each of the ITIL Service Management best practices, it becomes vitally important to understand how our Customer's requirements for those same practices in their IT service management environment. For custom engagements, AT&T can align with the Customer's application of the ITIL best practices.

The itSMF (owner of the ITIL Service Management best practices) has established a certification schema for individuals – not organizations. Within AT&T's Customer Care organization, AT&T has certified ~100 key individuals from world-wide Customer Care organization involved in implementation of AT&T's approach to ITIL.

ITIL® is a framework of best practices for delivering high-quality IT services. We take a disciplined approach in each area of the best practices in order to continuously improve processes within our service management organization. As part of that approach, we follow the IT Service Management Forum (itSMF) certification schema, which is a rigorous program for certifying individuals, rather than entire organizations.

We also follow these ITIL® service support practices:

- Configuration Management—through our BusinessDirect℠ portal, we provide tools that allow customers to review their inventory of service components.
- Incident Management—our help desk proactively detects and resolves faults that affect our services.
- Problem Management—we treat any recurring problem as an escalated priority, and we perform root cause analysis to prevent future recurrence.
- Change Management—we have a strict change management process, which means that we implement changes within predefined maintenance windows or agreed-upon timeframes.
- Help Desk—we offer a help desk for all services, and you can reach us through a variety of means, including Web-based tools such as BusinessDirect℠, telephone, or email. For critical incidents, we inform customers of resolution progress.
- Release Management—we release and configure software that you purchase.

5. Organization Profile

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point- by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

AT&T Response:

AT&T has read, understands, and complies. Please see the following point-by-point responses to Section 7 of the RFP.

7 ORGANIZATION AND STAFFING

7.1 (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.

AT&T Response:

AT&T will provide a Contract Manager as the single point of contact for the management of the NASPO ValuePoint Master Agreement. The proposed Contract Manager's contact information is below:

- Rick Frankhuizen
  AT&T Senior Contract Manager
  Email: rickf@att.com
  Telephone #: 661-263-9835
  Business Hours: 8:30 am – 5:30 pm (PT)

Please note: AT&T reserves the right to substitute or replace the proposed contract manager over the term of the contract with someone of similar qualifications as necessary for business or personal reasons and will provide reasonable notification should AT&T make this change.

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.**

AT&T Response:

AT&T will provide a Contract Manager as the single point of contact for the management of the NASPO ValuePoint Master Agreement. The AT&T proposed Contract Manager is a full-time employee and is an expert in negotiating, developing, and maintaining numerous types of standard and custom contracts including extensive experience with state and municipal governments. We include the proposed Contract Manager's resume below.

Please note: AT&T reserves the right to substitute or replace the proposed contract manager over the term of the contract with someone of similar qualifications as necessary for business or personal reasons and will provide reasonable notification should AT&T make this change.

RICK FRANKHUIZEN
AT&T SENIOR CONTRACT MANAGER
EMAIL: rickf@att.com
TELEPHONE #: 661-263-9835
BUSINESS HOURS: 8:30 AM TO 5:30 PM (PT)

SUMMARY

Consistent record of outstanding performance in a wide variety of positions and job responsibilities. Possess a high degree of business acumen and ability to make quick, accurate decisions. Able to work well in a collaborative team environment. Outstanding execution skills. Highly effective communication skills. Uniquely skilled in the following Contract Management areas:

- → Expertise in developing contracts using standard templates and custom documents
- → Exceptional negotiation skills
- → Substantial knowledge of legal terms and conditions
- → Experience in handling client contract-specific concerns related to contract management
- → Ability to manage multiple projects in a fast-paced, frequently changing, environment
- → Strong ability to work within a team environment, securing buy-in and agreement through collaborative efforts
- → Exceptional communication skills, both written and oral
- → Exceptional leadership skills
- → Understanding of the timing and cycles of contract negotiations

PROFESSIONAL EXPERIENCE

AT&T Inc.

Senior Contract Manager
2010 to present

- Support GEM (Government, Education and Medical) accounts for development of custom contracts, including large and medium sized account teams and customers
- Manage account negotiations and contract creation for multiple large opportunities during this period
- Extensive experience with AT&T suite of managed service offerings, Consulting, and wireline services.

- Conducted proposal preparation, contract review and negotiation, contract administration and customer contact activities to provide for proper contract acquisition and fulfillment in accordance with company policies, legal requirements, and customer regulations
- Advised management of contractual rights and obligations, and identify areas of contractual risk while using independent judgment and analysis of significant issue identification and resolution.
- Initiate, negotiate, review and approve for execution a wide range of contractual documents and agreements including government and commercial contracts as well as cooperative agreements
- Actively seeks guidance, consultation, and approval with other members of the contracts team, legal team, business owners, and other departments as needed to ensure compliance, customer satisfaction, and cost effectiveness.
- Perform contract actions that may be non-routine and require specialized techniques to accomplish business goals and objectives
- Respond to internal and external requests for contract information.
- Collaborate with support staff to ensure that program and market leaders are aware of financial status, program risk factors, reporting requirements, deadlines, compliance requirements, etc.
- Coordinate with accounting on project and system set-ups, contract billing and reporting, audits
- Perform proposal and contract management in a fast paced environment

Business Development Manager
2004 to 2010
1996 to 2002
Supported the Los Angeles Premier (Fortune 1000-sized) Accounts Sales Center. Responsibilities included development of sales strategy with account teams, contract negotiations with major customers, identifying and procuring internal resources required for special project requirements, revenue quota attainment, price management, sales force training and motivation.

- Helped deliver positive revenue growth for five out of the past six years, despite negative growth in corresponding AT&T market segment nationwide
- Achiever's Club (top 5% nationwide) in 1999, 2001, 2004 and 2005
- Experienced in entire range of AT&T products and services - IP, Wireless, Managed Security Services, traditional voice and data
- Direct negotiation experience with C-level clients as well as outside consultants, resulting in numerous large sales ranging up to $40+ million in annual revenue

Sales Manager
2002-2004
Managed a group of eight sales people, with account base of 50 clients and total billing to AT&T of approximately $40 million annually. Drove 45% increase in sales quota attainment and funnel management activities as compared to previous year.

International Network Architect
1995-1996
Provided pre-sale applications and technical support to Data Networking Account Executives for international data communications projects. Was responsible for understanding of customer data processing environment, evaluation of alternative network solutions and technical assurance of proposed design. Increased the sales of global Frame Relay and IP-based services by 75% during this period.

Data Networking Account Executive
1994-1995
Responsible for selling the complete line of AT&T Business Multimedia Services. Sold large international private line network to major manufacturer with facilities in China, Australia and throughout Europe. Developed and sold complex hub-and-spoke network for a nationwide bank with retail operations in over 25 states.

- Achieved 122% of Quota in 1995, 129% in 1994 and 105% in 1993.
- Achiever's Club in 1993, 1994 and 1995.

Technical Support Specialist
1990-1993
Responsible for technical sales and implementation support for the Sales Branch. Simultaneous management of multiple large, complex projects and sales efforts.

- Achiever's Club in 1991 and 1992.
- Leader's Council recognition (Top 1% of the sales force worldwide)) in 1993.

Education

1975	Stanford University	Bachelor of Arts Major in Economics	California State Scholarship Recipient
1980	UCLA Anderson School of Management	Master's in Business Administration Marketing	Member, Beta Gamma Sigma, National honorary association of business students

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.

AT&T Response:

The AT&T Contract Manager will be responsible for the following activities.

- Single contract management point of contact for NASPO Valuepoint
- End-to-end contract management including master agreement, participation addendums, and product addenda
- Lead contract development manager on State- and Agency-level participating addendums
- Contract subject matter expert for internal AT&T sales and marketing personnel
- Participation in NASPO annual meetings

6. Technical Response

This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

AT&T Response:

AT&T understands and complies.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror’s should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

AT&T Response:

AT&T understands and complies. Please refer to the following point-by-point responses to Section 8 of the RFP.

8 TECHNICAL REQUIREMENTS

If applicable to an Offeror’s Solution, 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 Solution 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.

AT&T Response:

AT&T understands and complies. We provide our point-by-point responses to each technical requirement below.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service uses a SaaS cloud service model. Users have the ability to access software applications which enable communication, collaboration, and conferencing with one or more other users via audio, video, graphic, or text interactions. Applications are accessed via clients installed on users' PC, tablet, or mobile devices. AT&T hosts and manages the solution, which includes a 24x365 customer service and technical helpdesk.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	AT&T Video Meeting with Blue Jeans has three different SaaS models that are sold through AT&T systems: • Named Host - licensing a specific user for a Blue Jeans account • Virtual Ports - Concurrent port usage with ability for all users to access • PrimeTime - large event web service that can have 3,000 participants with video capabilities
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service uses a SaaS cloud service model.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	Yes	This service is implemented via tools and processes “within the cloud” and hence regarded as being most closely associated with “infrastructure.”
AT&T Unified Communications as a Service	SaaS	Yes	AT&T Unified Communications (UC) Voice service uses a SaaS cloud service model. Users have the ability to access software applications which enable communication, collaboration, and conferencing with one or more other users via audio, video, graphic, or text interactions. Applications are accessed via clients installed on users’ PC, tablet, or mobile devices, or via specialized devices (e.g., telephone stations) deployed

AT&T Product	Category	Comply (yes/no)	AT&T Response
			by the customer for that purpose. AT&T UC Voice uses a hybrid cloud deployment model. The service is primarily offered via a private cloud model where an MPLS network service such as AT&T VPN is used to connect customer sites to the cloud platform. However, service may be extended to remote users via a public cloud model to reach broadband Internet endpoints.
AT&T Hosted Contact Center Service	SaaS	Yes	Comply
AT&T Premises-Based Firewall Service	IaaS	No	AT&T Managed Intrusion Protection/Detection service does not directly meet many of the requirements as presented because it is a managed service versus a contemporary cloud service. As security is listed in the definition of cloud services, it is our intent to present these services for NASPO consideration even though they do not directly map to the requested cloud services.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	No	AT&T Managed Intrusion Protection/Detection service does not directly meet many of the requirements as presented because it is a managed service versus a contemporary cloud service. As security is listed in the definition of cloud services, it is our intent to present these services for NASPO consideration even though they do not directly map to the requested cloud services.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	AT&T Content Delivery Network Service (ACDN) provides cloud based services with no additional, on-site equipment required. There are also no additional or hidden charges to consider when purchasing ACDN services. Various facets of the service can include: • IaaS Services: Web Content Delivery – Standard Secure-industry leading web performance solution makes web experiences fast, reliable, and secure across all end-user situations, while maximizing infrastructure offload and operational agility. • Cloud DNS Services- Fast DNS-DNS resolution, coupled with Global Traffic Manager • IaaS/Security/Web Security - Kona Site Defender (KSD)-Defends against all types of

AT&T Product	Category	Comply (yes/no)	AT&T Response
			DDoS, web application and direct-to-origin attacks. • Kona Rule Update Service-Security support for KSD. Client Reputation – Defends against application layer and DDoS attacks by identifying malicious IP addresses dynamically and risk scoring the IPs.

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:

AT&T Response:

Where applicable, all of our services are compliant with NIST standards due to our extensive security engagements with Federal Agencies, State Agencies across the United States, and large enterprise customers with strict requirements for NIST compliance.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service provides On-Demand and Self-Service capabilities. This service enables users to initiate and terminate communications with other users on demand, no scheduling is required for any resources. Customers may also add new users via a self-service portal.
AT&T Video Meetings with Blue	SaaS	Yes	Customer admins are able to assign Blue Jeans accounts to users and remove those as needed, end

AT&T Product	Category	Comply (yes/no)	AT&T Response
Jeans			user modifications are available as well.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is an on-demand web filtering and security service that allows for customer use to scale over time. Human intervention is not necessary between the customer and Blue Coat when ramping up the service to full use as there is buffer built into the service that is constantly monitored and adjusted as volume of traffic increases.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS Service is not an "on Demand" service in the context of NIST Characteristics. It is a "setup and maintain" service in which the purchasing entity contracts for the service over a period of time, interacts with a 24x7 Support Team to maintain sensitivity levels of the DDoS serivce, and monitors reporting activity of the Service.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Voice provides On-Demand and Self-Service capabilities. The service enables users to initiate and terminate communications with other users on demand – no scheduling is required for any resources. Customers may also add new users via a self-service portal without requiring provisioning activity by AT&T.
AT&T Hosted Contact Center Service	SaaS	N/A	1) User/agent administration of access is self-service. The inContact platform is completely roles and permissions-based, to the individual user level. inContact Central, our web-based administration hub, provides administrators with the ability to add/modify/ remove users, change granular permission levels for access, and easily create security profiles and groups for ease and flexibility in platform administration. 2) Customer call recording data access is self-service by this same administrative access. 3) Retrieving and removing call recordings from the system is self-service. The customer must interface with inContact to set this option, but once set, transmission of data is customer controlled.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN's Luna portal practically allows for anything to be self-serviceable from the Akamai Web Performance and Web Security product suites. Users can either login into Luna or take advantage of the available APIs to achieve the required functionality. And finally, they can also build their own custom APIs to interface with the ACDN platform.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service offers Broad Network Access. This service can be supported any broadband Internet connection.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans solution works over the Internet, MPLS, or mobile networks and can be accessed through a variety of endpoints.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service supports many different location specific connection types as well as direct connections to many devices. This allows for filtering and security to be provided all devices connected to a network location, and a majority of mobile devices that are used for accessing the web.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	AT&T DDoS Service, to the extent that Customer's access the DDoS Threat Portal from a broad variety of devices and browsers, complies with the characteristic.
AT&T Unified Communications as	SaaS	Yes	AT&T UC Voice offers Broad Network Access. AT&T MPLS services used to access UC Voice are provided at thousands of access points in the US and in other

AT&T Product	Category	Comply (yes/no)	AT&T Response
a Service			countries. These services may also be extended to any broadband Internet connection through the use of an AT&T Network-based Remote Access service.
AT&T Hosted Contact Center Service	SaaS	N/A	This cloud service is a call contact management system, and designed to work from a typical call contact agent environment, with a regular CPU connected through a software driven VoIP phone. Therefore, the classic definition of Broad Network Access does not apply. It is accessible through a windows operating system. That said, there does exist an administrative access through iPad technology, but this does not allow agent access for receiving and sending phone calls.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN conforms to the Broad Network Access methodology for authorized users. The broad network access characteristic of the cloud makes it easy to take advantage of high-speed networks, fast DNS services, and CDN services of Akamai to speed up your application. This is especially important for mobile applications, where networks are slower, making every byte or millisecond of latency count. Akamai can help cache content closer to the end-users, compress content, and make sure it supports conditional requests. All of these can significantly speed up the customer's website.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service utilizes Resource Pooling. This service uses pooled processing, memory, storage and network resources to enable users to communicate with one another. While the service is offered using platform equipment in specific AT&T data centers, users are unaware of any particular element that handles a given interaction or that provides a supporting function (e.g., administrative changes) for their service.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	The service was built from the ground up by Blue Jeans and consists of software that runs on cloud-compute clusters from a leading global server vendor. The service is hosted in multiple tier-4 co-location data centers around the world, and in each of these PoPs, dedicated cages that only Blue Jeans personnel have access to and are protected with 24x7x365 security and multiple levels of biometric access controls.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is a multi-tenant SaaS platform that shares resources of its global footprint between customers. Resources are moved around within the service infrastructure in order to deal with customer demand and create a seamless user experience. However, based on customer request and to abide by data storage regulations, customers can be manually configured to have all web filtering, security, and reporting storage reside in specific locations.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Voice utilizes Resource Pooling. The service uses pooled processing, memory, storage and network resources to enable users to communicate with one another. While the service is offered using platform equipment in specific AT&T data centers, users are unaware of any particular element that handles a given interaction or that provides a supporting function (e.g., administrative changes) for their

AT&T Product	Category	Comply (yes/no)	AT&T Response
			service.
AT&T Hosted Contact Center Service	SaaS	Yes	The inContact ACD application is scaleable within limits determined by design and contract. This platform depends on pooled resources such as database, switching equipment, web services, and certain customizable configurations.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	The ACDN platform is the largest distributed platform in the world, and hence confirms to the Resource Pooling methodology of NIST. ACDN's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., region). Examples of resources include storage, processing, memory etc.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx

AT&T Product	Category	Comply (yes/no)	AT&T Response
with Cisco WebEx			Service exhibits Rapid Elasticity. Capabilities and resources to enable user interactions are assigned by AT&T as interaction requests occur. Additional ports are provided during periods of high demand than during those of low demand. Individual users are unaware of demands from other users and from an individual perspective the service appears to have unlimited capacity.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Customer admins are able to assign Blue Jeans accounts to users and remove those as needed, end user modifications are available as well. Ports model customers are able to burst over the allotted ports for the day so that they can meet their requirements.
AT&T Cloud Web Security Service	IaaS	Yes	The capabilities of the cloud service appear to be unlimited to the AT&T Cloud Web Security Service is not currently automatically elastic, however features and functionality associated to elasticity are being built into the service infrastructure - some complete and some in progress. Additionally, due to the immediately available access to all global AT&T cloud infrastructure facilities, manual changes can easily be made to accommodate elasticity.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	To the extent that DDoS "scales up" and a DDoS attack occurs, that it the only scenario in which DDoS relates to NIST Elasticity.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Voice exhibits Rapid Elasticity. Capabilities and resources to enable user interactions are assigned by UC Voice as interaction requests occur. Messages are delivered to users and calls are set up and torn down as users request them, so more capabilities are provided during periods of high demand than during those of low demand. Individual users are unaware of demands from other users and from an individual perspective the service appears to have unlimited capacity.
AT&T Hosted Contact Center Service	SaaS	See Comment	Depends on agreed definition of 'rapid elasticity.' the inContact ACD service is elastic to the extent of planning and design. inContact maintains a capacity management staff and plans sizes systems according to customer requirements and expert professional services. Some of this capacity management is automated, and some determined by design.
AT&T Premises-Based Firewall	IaaS	See Comment	Not applicable

AT&T Product	Category	Comply (yes/no)	AT&T Response
Service			
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN is capable to scale to the millions of additional user requests for delivery and storage.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service provides Measured Service through metering of resources at the user account level. The pricing structure is fundamentally per-user, per-month with the charge for web conferencing and per minute, per participant for audio conferencing.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans uses active user accounts to measure the cost of the service to the customer. Both ports and named hosts services have a monthly cost which is able to be modified as needed and billed accordingly.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service fulfills all requirements outlined in the characteristic definition outlined in appendix D for SaaS.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service
AT&T Unified	SaaS	Yes	AT&T UC Voice provides Measured Service through

AT&T Product	Category	Comply (yes/no)	AT&T Response
Communications as a Service			metering of resources at the user account level. The pricing structure is fundamentally per-user per-month with the charge based on the level of functionality and optional features to which the user subscribes.
AT&T Hosted Contact Center Service	SaaS	< Select >	inContact measures and monitors its services, focusing on ACD and Workforce Optimization, both for individual customers and overall security, reliability and performance. Billing is based on metered usage of telecom and data services. Storage is based on metered usage.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN meets this characteristic by defining service agreements, monitoring its cloud services, supporting planned/paid audits etc.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service is one of multiple SaaS offerings provided by AT&T. It primarily addresses the "Collaboration" sub-category, but also provides attributes of the "Meeting Planning, hosting, conferencing" sub-category. AT&T hosts and manages the solution, which includes a

AT&T Product	Category	Comply (yes/no)	AT&T Response
			24x365 customer service and technical helpdesk.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a cloud based service that has many use cases from education, consulting and judicial testimony. There are many use cases that can meet the services of the NASPO participants.
AT&T Cloud Web Security Service	IaaS	Noted	AT&T Cloud Web Security Service is offered as SaaS in the area of Security and provided for all areas within the service category and for all entities within an organization.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	Noted	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Voice is one of multiple SaaS offerings provided by AT&T. It primarily addresses the "Collaboration" sub-category, but also provides attributes of the "Meeting Planning, hosting, conferencing" sub-category.
AT&T Hosted Contact Center Service	SaaS	Yes	Comply
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Noted	The services that ACDN offers can be divided into the following solution areas: Web Acceleration, Media Delivery, Web Security and Data Center Security.

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

AT&T Response:

AT&T understands. AT&T has categorized each of its services using the three categories requested by NASPO and as described in Attachment C (i.e., SaaS, Paas, and IaaS). It should be noted that many of our services don't fall completely or cleanly within any single category. These categories aren't completely applicable for some of the services that we are proposing. We have categorized our services based on "best fit." For ease of review, we typically included the category names along-side each product name in tables throughout the proposal.

AT&T has also reviewed the data risk classifications described in Attachment D. AT&T understands the concerns that virtually all of our customers have regarding the care of data that may reside in or be operated upon within our various services. We handle all data entrusted to us by customers carefully and thoughtfully. Using FIP Publication 199 as a guide, we have reviewed the particular services offered in this proposal and have determined that the most appropriate category of data risk would be "Low Risk Data."

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.

AT&T Response:

AT&T has also reviewed the data risk classifications described in Attachment D. AT&T understands the concerns that virtually all of our customers have regarding the care of data that may reside in or be operated upon within our various services. We handle all data entrusted to us by customers carefully and thoughtfully. Using FIP Publication 199 as a guide, we have reviewed the particular services offered in this proposal and have determined that the most appropriate category of data risk would be "Low Risk Data."

Please refer to the AT&T response provided for RFP Section 6.7 ("Best Practices") for additional commentary.

8.2 (E) SUBCONTRACTORS

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing

all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for AT&T Conferencing with Cisco WebEx.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans has strategically partnered with AT&T to provide a robust network partnership that allows customers a secure and robust connection between Blue Jeans over an MPLS or public Internet connection.
AT&T Cloud Web Security Service	IaaS	Noted	AT&T Cloud Web Security Services is delivered under the control of AT&T service delivery and subcontractor agreements do not apply.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T does not intend to use subcontractors to perform contract requirements for DDoS.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for UCaaS.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact will deliver a true cloud/SaaS solution, utilizing no subcontractors. All implementation, training, and ongoing support will be provided by US domestic inContact employees.
AT&T Premises-Based Firewall Service	IaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for our Premises-Based Firewall Service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for our Managed Intrusion Detection/Intrusion Prevention Service.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN service is provided in conjunction with AT&T's supplier Akamai. AT&T and Akamai enjoy a strong working relationship. AT&T's value proposition includes: • Trusted account team and support services • Dedicated Client Tech Lead (CTL) • Dedicated Client Executive (CX) • Tier 1/2 support services provided by AT&T personnel Under our agreement with Akamai, AT&T provides 7x24 support for all AT&T CDN products through the AT&T branded LUNA customer portal, for timely resolution of customer issues. E-bonding synchronizes ticketing activity between AT&T and Akamai,, and we have direct channels to Akamai support for issues requiring additional expertise.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for AT&T Conferencing with Cisco WebEx.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans does not use sub-contractors.
AT&T Cloud Web Security Service	IaaS	Noted	AT&T Cloud Web Security Services is delivered under the control of AT&T service delivery and subcontractor agreements do not apply.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS Service is owned/controlled by AT&T. No third party vendors have access.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T does not intend to use subcontractors to perform contract requirements for UCaaS.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact will deliver a true cloud/SaaS solution, utilizing no subcontractors. All implementation, training, and ongoing support will be provided by US domestic inContact employees. No subcontractors will be used in the delivery of our solution or services
AT&T Premises-Based Firewall Service	IaaS	Yes	Subcontractors are only used for onsite deployment of the premise portion of the service and for hardware repair/replacement. However this partner is an established AT&T vendor worldwide.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Subcontractors are only used for onsite deployment of the premise portion of the service and for hardware repair/replacement. However this partner is an established AT&T vendor worldwide.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	AT&T provides ACDN service in conjunction with our supplier Akamai. Akamai does not use subcontractors.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

AT&T Response:

AT&T selects its subcontractors with the goal to provide the best service to you.

AT&T may subcontract work to be performed under an agreement, but shall retain full responsibility for all such work, including any obligations it performs through its subcontractors. AT&T shall be solely responsible for payments due its subcontractors.

We use skilled subcontractors and remain fully responsible for the work they do for you.

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.

AT&T Response:

Response timeframes vary by individual customer requirements. Estimated processes and timelines can take from 30 days to 90 days to implement based on the service AT&T provides and customer requirements. AT&T will assign a Project manager and provide communication via conference calls and email to notify when services will be completed.

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.

AT&T Response:

AT&T does not typically push adware within private customer portals. However, for public web sites, AT&T reserves the right to insert targeted ads and banners pertaining to the service being delivered.

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

AT&T Response:

User test/staging environment is not applicable for the products we propose in this response.

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.

AT&T Response:

AT&T complies with all applicable federal, state, and local laws. As such, AT&T complies with access attributes specified by the Americans Disability Act. AT&T designs all software interfaces with an eye toward being ADA compliant.

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.

AT&T Response:

AT&T makes every attempt to keep its software interfaces compatible with mainstream versions of the major browsers and/or applicable client software.

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.

AT&T Response:

It is incumbent on Purchasing Organizations to apprise AT&T of intended uses involving highly sensitive data. In those cases, AT&T may advise the inclusion of additional layers of data protection (e.g., encryption).

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

AT&T Response:

Because AT&T is proposing a broad range of services, it is not feasible at this stage to generate a sample timeline.

AT&T will assign a project implementation manager to assist with onboarding of major projects. One typical deliverable in such cases is a detailed project plan with formal tracking of people, timelines, and dependencies. For "self-service" types of services, such project management is not applicable.

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).

AT&T Response:

Quality Assurance

Our quality assurance program encompasses numerous quality standards. Certification dates vary greatly based on the standard and the department within AT&T.

We have been International Organization for Standardization (ISO) certified since 1996 and received our first TL 9000 certification in 2004. We employ ISO standards continually to maintain performance excellence and improve our execution capabilities on a global level.

Achieving compliance with the ISO standards builds discipline into our management system which contributes to our ability to meet or exceed our customers' expectations.

ISO developed the ISO 9001 and ISO 9004 standards to be parts of a consistent quality management system. These guidelines provide ways for organizations to achieve excellence through continual improvement in the performance of their business.

The ISO 9001 standard defines a basic set of requirements for a quality management system. The ISO 9001:2000 standard has a strong focus on customer satisfaction and continual improvement. The standard emphasizes the use of data on products and processes to define opportunities for improvement. The standard contains a process model concept that is very similar to the Plan-Do-Check-Act cycle and the Baldrige Model.

AT&T strictly adheres to achieving the highest levels of quality in the four main clauses of ISO

- Management responsibility
- Resource management
- Product realization
- Measurement, analysis, and improvement

Beyond our ISO and TL 9000 certifications, we have departments that follow Six Sigma and in our IT department, ITIL and CMM efforts are underway.

AT&T's processes and policies generally fulfill the security and incident management aspects of the Information Technology Infrastructure (ITIL) and the ISO27000 (formerly ISO 17799) standards. ISO is incorporating the security components of the ITIL library, a comprehensive collection of best practices for IT service management, into the new ISO 27000 series. This series consolidates all security sections from previous ISO standards.

It is our goal to consistently improve our business processes and improve our client satisfaction.

Escalation Plan

To escalate a trouble report to resolve an issue with your AT&T services, we use a formal procedure that depends on trouble severity.

Once we've identified a problem or you've reported one via our 24x7 Global Customer Support Center (GCSC) helpdesk, we follow specific timelines and escalation paths. These intervals and paths—which vary according to the severity of your service trouble—help ensure that we engage the right resources to resolve the issue.

We define service trouble as having one of three severity codes:

- Severity 1 (critical problem)—The network or application is unusable (i.e., recovery or bypass is impossible), and you're unable to work.
- Severity 2 (major problem)—The problem creates a severe impact on your business but doesn't stop service functions, or you've found a way to bypass the issue and conduct business.
- Severity 3 (minor problem)—The problem has minimal impact on your business, so creating an alternate way to conduct business is unnecessary.

After we determine a severity code, we follow a timeline to progressively escalate the issue until we resolve it. This process may involve the actions of team members that range from local managers to our global services executives.

The escalation path includes

- 1st Level—24x7 Global Associate
- 2nd Level—24x7 Team Leader
- 3rd Level—Operations Manager
- 4th Level—Global GCSC Director
- 5th Level—Global GCSC AVP

See below table for a timeline of standard escalation intervals for severity 1 and 2 troubles.

Timeline for 'Time to Restore'	Severity 1 (target = 4hrs)	Severity 2 (target > 4hrs)
Creation of Ticket & Problem Determination	0 - 120 min (0 - 2hrs)	0 - 240 min (0 - 4hrs)
Escalate to Level 1	at 120 min (2hrs)	at 240 min (4hrs)
Escalate to Level 2	at 240 min (4hrs)	at 480 min (8hrs)
Escalate to Level 3	at 360 min (6hrs)	at 720 min (12hrs)
Escalate to Level 4	at 480 min (8hrs)	at 960 min (16hrs)
Escalate to Level 5	at 600 min (10hrs)	at 1200min (20hrs)

The table above provides standard escalation intervals.

We may negotiate non-standard intervals where circumstances such as an executive escalation, customer demand, significant business impact, critical site involvement, or

sensitive customer status dictate faster or slower escalation to resolve the fault/trouble report. In each case, we investigate the requirement to escalate before taking escalation action

These procedures address acute service issues. In addition, your account and service managers will work with you during your regular stewardship review meetings to identify and escalate chronic service issues.

This means that we use all applicable resources to resolve any service issue.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

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

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

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

AT&T Response:

AT&T understands and complies. AT&T provides an AT&T account team that executes each addendum for customer purchases. Additionally, AT&T provides ongoing support for all proposed services.

AT&T Service Level Agreements are contained within the applicable Service Guide. Please refer to Attachment C for the AT&T Service Guides with SLAs.

The following table outlines any product specific responses to the requirements above.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Live 24x7 Help desk support for both audio and WebEx suite of applications Dedicated account manager as a

AT&T Product	Category	Comply (yes/no)	AT&T Response
			single point of contact Full escalation paths for Sales, Customer Service and Maintenance Support available by phone, email, and trouble ticketing system Support is via phone or chat.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	AT&T Video Meetings with Blue Jeans has 24x7 Support which can be accessed at www.bluejeans.com/contact or by dialing 1-800-403-9256. http://bluejeans.com/support/advanced-services. Furthermore, based on certain criteria of the customer, Blue Jeans will offer a dedicated Customer Success Manager as an additional resource to assist as a point of contact, training and deployment.
AT&T Cloud Web Security Service	IaaS	Yes	a) AT&T Account Managers (if one is assigned) serves as lead representatives for their assigned customers. b) As a member of the AT&T community, we provide you multiple ways to interact or contact us in order for us to provide the support you need to get the most out of your AT&T investment: • Phone: Access to technical support 24x7 and administrative / non-technical support is available during normal business hours Monday-Friday • Web: Access to the resources on online for support • E-mail: Assistance for non-technical issues, such as licensing, entitlement, or BTO login, or general service inquiries c) AT&T understands and will comply d) AT&T will work with customer to select most appropriate options and feature based on customer requirements. e) AT&T will work with customer to provision service.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	
AT&T Unified Communications as a Service	SaaS	Yes	a) AT&T will assign an account manager as the lead representative for each entity that executes a Participating Addendum and will keep contact information current. b) For each cloud service, you receive base support without additional cost. Base support provides cloud users with various 24x7 web-based support and

AT&T Product	Category	Comply (yes/no)	AT&T Response
			technical resources via our Cloud Portal. Portal resources include • Access to our guides and documentation • Demos and tutorials • FAQs and technical specification information • Developer forums and wikis • Unlimited trouble and incident ticketing submissions You can receive enhanced support for an additional monthly charge per user. This fee-based support covers all cloud services you currently have and any others you add in the future. In addition to the online resources you get with base support, enhanced support provides access to our cloud services technical support team, which is available 24x7 via phone and email to answer your questions. So, you have easy access to the support you need to manage your cloud-based services. c) AT&T Complies and provides a 24x7 helpdesk to provide immediate assistance with inquiries. d) AT&T provides design services to assist customers with setup and operation of UC Voice and with configuration of network services and other components that may be used in conjunction with UC Voice (e.g., equipment at the customer's premises to provide survivable communications). e) AT&T provides installation services for UC Voice and other components that may be used in conjunction with it.
AT&T Hosted Contact Center Service	SaaS	Yes	Supported with our Proposed Customer Support Package.
AT&T Premises-Based Firewall Service	IaaS	N/A	
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	N/A	
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network	IaaS	Yes	24x7 support through an express routing code is available with the premium support option. The

AT&T Product	Category	Comply (yes/no)	AT&T Response
Service			named enhanced support option provides for • High availability and business continuity • Faster, prioritized 24x7 access to Akamai Support • Continuous proactive engagement for periodic reviews and best practice recommendations. Response time SLAs for enhanced support are: • Critical Impact (P1) <=30 minutes • High Impact (P2) < =2 hours • Low Impact (P3) <= 1 business day. Design and Installation/Integration services are available for all service offerings.

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.

AT&T Response:

Protect Data

AT&T secures and protects customer data by using expert skills and advanced technology.

We implement our security policy through initiatives, processes, and procedures that our security organizations administer worldwide. Each region executes these ongoing program initiatives.

We use security mechanisms to

- Control and validate access
- Protect the network perimeter
- Detect intrusions
- Test for vulnerabilities
- Manage workstation security

- Disseminate security advisories
- Conduct periodic security awareness training

We work with you to assess your information security policies, and we recommend changes to them when we implement your service. Once you accept the service, you can request changes to security policies through the Move, Add, Change, and Delete (MACD) tool in AT&T BusinessDirect®. AT&T does not share customer-specific, sensitive, or proprietary information.

So, we work with you to establish the appropriate security policies to protect customer data.

Dispose Data

The AT&T Records & Information Management (RIM) organization properly disposes of information.

The objectives of the RIM organization and the associated RIM components are to enable AT&T to create and manage authentic, reliable, and useable records. These records should support business functions and activities for as long as they are required to comply with all legal and regulatory recordkeeping requirements.

AT&T is committed to the development and application of sound records and information management practices.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T secures and protects customer data by using expert skills and advanced technology. We implement our security policy through initiatives, processes, and procedures that our security organizations administer. We use security mechanisms to: • Control and validate access • Protect the network perimeter • Detect intrusions • Test for vulnerabilities • Manage workstation security • Disseminate security advisories • Conduct periodic security awareness training

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a SaaS based company, our web site is maintained internally and each enterprise will have users assigned different roles which provide for different views and edit abilities. Blue Jeans operates a multi-tenant environment with logical separation between enterprise accounts. Data is logically separated between clients within the environment based on Enterprise IDs. As a standard, Blue Jeans restricts access to the production environment to only those employees with a job function(s) that requires access. All user accounts access are secure using the following technologies and security measures: • Standard user accounts or admin user accounts • Each Blue Jeans account is secured with a standard user name and password • Authentication requests are always sent over HTTPS • Passwords are SHA-256 salted/hashed in the database and can never be viewed in plain text • Passwords are never sent via email or any other form of electronic transmission (the "Forgot Password" feature only allows for resetting the end-user's password) Blue Jeans uses an overwrite method using /dev/zero with a single pass for devices that will leave the organization that are functioning, storage devices that are not functioning when a system is retired are removed from the device and stored until they can be properly destroyed. Blue Jeans helps ensure that storage media containing customer data is properly sanitized of all customer information in accordance with applicable laws and regulations prior to disposal or reuse for non-Blue Jeans processing.
AT&T Cloud Web Security Service	IaaS	Yes	All customer WebTraffic is encrypted in transit and all log files can be encrypted at rest. WebTraffic Reporting log deletion is configurable on a per customer basis via the Cloud Security Portal. Upon expiration of contract services, all WebTraffic Reporting logs, all policies, and any associated customer configuration information is deleted no later than 60 days after the day of expiration, however it can be deleted sooner if requested.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS does not retail data, except to the extent provided in reports, which are accessible through the BusinessDirect Portal and controlled by the Customer.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T secures and protects customer data by using expert skills and advanced technology. We implement our security policy through initiatives, processes, and procedures that our security organizations administer. We use security mechanisms to: • Control and validate access • Protect the network perimeter • Detect intrusions • Test for vulnerabilities • Manage workstation security • Disseminate security advisories • Conduct periodic security awareness training The data storage used by AT&T UC Services is designed to maximize data confidentiality, data integrity, and availability. Separate and dedicated data storage volumes are used for each deployed AT&T UC Services application. The data within these volumes is not accessible via other AT&T UC Services or non-UC Services applications; even access to the operating system for customer specific AT&T UC Services applications is limited to the manufacturer (Cisco). AT&T UC Services supports the option to record and store voicemail messages for compliance via third party applications. Access to voicemail messages is protected by user-based usernames and passwords; others do not have access to these messages.
AT&T Hosted Contact Center Service	SaaS	Yes	Security is very important at inContact and as such inContact customers' access data and administration of the platform through a cloud interface. In this multi-tenant environment, customers are not allowed to directly access inContact's databases. Security on applications which customers will have access to will include application password encryption by means of salted hashes, and access links to inContact via https:// and/or SSL. Typically customers use the http:// url and inContact does a redirect to the HTTPS site. inContact implemented a robust layered security policy on all IP POP elements including but not limiting to:

AT&T Product	Category	Comply (yes/no)	AT&T Response
			• User access controls utilize a user/password login, where users are in turn controlled via a roles based permissions model that is client administered and configurable. • Web servers are in firewall secured DMZ's • IDS/IPS systems monitor intrusion activities and prevent penetration • Regular vulnerability scans and penetration tests are performed • Anti-virus is deployed on all systems • inContact utilizes Sonus SBCs; an SBC is essentially a VoIP firewall • inContact offers an MPLS solution to allow the creation of a 'private' network for VoIP traffic We also perform quarterly and yearly audits, a yearly SSAE 16, SOC2 report and we obtain assurances such as a SAS70/SSAE 16 or Vendor Security Questionnaire from all of our facility vendors.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Client data is not held within AT&T Premises-Based Firewall Service. However to secure the operational systems of the service we implement our security policy through initiatives, processes, and procedures that our security organizations administer. We use security mechanisms to: • Control and validate access • Protect the network perimeter • Detect intrusions • Test for vulnerabilities • Manage workstation security • Disseminate security advisories • Conduct periodic security awareness training
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Client data is not held within AT&T MIDS/MIPS Service. However to secure the operational systems of the service we implement our security policy through initiatives, processes, and procedures that our security organizations administer. We use security mechanisms to: • Control and validate access • Protect the network perimeter • Detect intrusions • Test for vulnerabilities • Manage workstation security

AT&T Product	Category	Comply (yes/no)	AT&T Response
			• Disseminate security advisories • Conduct periodic security awareness training
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	For data handling/protection, ACDN is fully compliant with FedRAMP standard of delivery, protection and storage.

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

AT&T Response:

AT&T adheres to all applicable federal, state, and local laws. AT&T retains a staff of attorneys and paralegals, many of whom "major" in particular products as well as others who focus particularly on higher order issues in the realms of security and privacy. These experts provide ongoing guidance to AT&T product managers throughout the life-cycle of each AT&T product or service.

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.

AT&T Response:

AT&T adheres to all applicable federal, state, and local laws. Additionally, AT&T has strict guidelines regarding the use and access protocols for all customer account information.

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.

AT&T Response:

All of our services are compliant with NIST standards due to our extensive security engagements with Federal Agencies, State Agencies across the United States, and large enterprise customers with strict requirements for NIST compliance.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Conferencing with Cisco WebEx is a SaaS service for Audio and Web Conferencing that meets the essential characteristics of the NIST definitions.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans uses standards based technology to connect various end points and software applications together jointly. Interoperability is at the fabric of Blue Jeans value to the market therefore NIST and standards based services are critical for success.
AT&T Cloud Web Security Service	IaaS	See Comment	AT&T Cloud Web Security services does not commit to comply with all areas of NIST. Additional cloud security certifications (including SSAE16 and ISO27001) will continue to be maintained.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T is committed to and in fact a co-author or contributor to many industry standards and compliance methodologies and will continue that effort
AT&T Unified Communications as a Service	SaaS	Yes	AT&T Unified Communications as a Service for hosted VoIP meets the essential characteristics of the NIST definitions.
AT&T Hosted Contact Center Service	SaaS	Yes	We help our customers design solutions that checks for compliance with the industry standards most important or applicable to their business. Below is a snapshot of our many certifications: PCI - We're designated as a Service Provider Level 2 and Merchant Level 3 for PCI (Payment Card Industry). That means we complete an annual self-assessment and attestation of compliance, quarterly vulnerability scans, and an annual penetration test and audit of the controls. Our Attestation of Compliance (AOC) is completed by our internal audit department which is certified as an Internal Security Assessor. inContact also supports configurations and contact

AT&T Product	Category	Comply (yes/no)	AT&T Response
			center requirements where some data considered by the customer as sensitive and may be present in portions of the contact data inside of the inContact Platform which require PCI level 1 compliance. These configurations typically involve deeper integration between platforms for increased efficiency and are typically instituted when the customer finds it necessary to process, transmit, or store sensitive data such as HIPAA information or cardholder data (CHD) outside of customer control. Because the data resides outside of customer control the customer must consider additional risks, and additional efforts in their platform design. inContact supports such configurations utilizing an optional enhanced PCI level 1 solution. SOC 2 Type II - In 2011, the American Institute of Certified Public Accounts (AICPA), the SAS 70 Audit was replaced by three new Service Organization Control (SOC) standards, SOC 1, SOC 2, and SOC 3. Since our services don't directly host or affect customers' financials, we completed a SOC 2 Type II report, which validates the effectiveness of our operating controls. 404 SOX - Our 404 Certification for Sarbanes-Oxley (SOX) designates us as an Accelerated Filer. Our IT security and controls are included in this annual certification to evaluate our controls over financial reporting. We protect private information like consumer or employee information (such as credit card numbers, name, social security number, and phone number). This audit is performed by our internal audit department and confirmed by external auditors, Deloitte & Touche. FCC and CPNI - We comply with all Federal Communications Commission (FCC) regulations including protecting Customer Proprietary Network Information (CPNI) which is data we obtain in the normal course of providing you with telecom services. This type information includes where, when and whom you call, and the types of service offering and products you get from us. Safe Harbor - As a Safe Harbor partner, we use the proper policies (privacy, network and computer security, hosting, and change management) and controls to help ensure storage and transmission of customer information internationally is secure

AT&T Product	Category	Comply (yes/no)	AT&T Response
			according to country regulations and industry best practices such as PCI, Safe Harbor and section 404 standards. We also complete an annual audit of compliance. Although some industry standards may not apply to our company, we take our customers' compliance needs seriously. Standards such as HIPPA (can provide a business associate agreement), GLBA, Dodd Frank and FDIC are similar and closely related to PCI, 404 and SOC requirements. We help our customers design solutions that help ensure compliance with the industry standards most important to their businesses. inContact provides encryption using an AES-256 compliant encryption to protect calls from unauthorized access, and provides the ability to not capture/automatically insert white noise when sensitive data is being captured by the agent.
AT&T Premises-Based Firewall Service	IaaS	See Comment	AT&T is committed to and in fact a co-author or contributor to many industry standards and compliance methodologies and will continue that effort. AT&T Premises-Based Firewall Service does not directly map to the standards as communicated in this RFP because it is a managed service versus cloud offering as defined in the RFP.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	AT&T is committed to and in fact a co-author or contributor to many industry standards and compliance methodologies and will continue that effort. AT&T Intrusion Detection/Prevention Service does not directly map to the standards as communicated in this RFP because it is a managed service versus cloud offering as defined in the RFP.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Maintaining security certifications is an on-going process. For any security compliance, AT&T and Akamai go through regular audits and accountings in order to maintain that particular compliance.

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.

AT&T Response:

AT&T's security policies align with International Standards Organization ISO 27001:2005 standards.

In 2011, we obtained certification of our compliance with this standard. See the following link for our ISO 27001 certificate and statement of applicability:

- http://cso.att.com/ISO27001/index.html

This means that we've successfully demonstrated our security controls to a third-party auditor.

PCI

As a certified Level 1 Merchant for its own credit card billing, AT&T is familiar with, subject to, and currently validated for the Payment Card Industry Data Security Standard (PCI DSS) requirements.

The PCI DSS is generally inapplicable to telecommunication service providers (i.e., transport-only suppliers). However, an industry-recognized Qualified Security Assessor (QSA) for PCI validated AT&T to enable its customers to meet their PCI obligations.

So, AT&T adheres to PCI standards.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Reservationless Audio Conferencing with WebEx Service adheres to security standards that match or exceed the best practices outlined by: • The Center for Internet Security • AT&T Labs, • AT&T Security Policy Requirements (ASPR), • Cisco Security. Also, effective June 15, 2011, the SAS 70 was replaced by the domestic US Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). The formal audit report

AT&T Product	Category	Comply (yes/no)	AT&T Response
			under the new standard is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1". The SOC 3 Report, also known as a SysTrust Report, covers the following principles—Application Services: Security, Availability and Processing Integrity; Enterprise Hosting: Security and Availability. This report is made publically available for distribution. PCI: As a certified Level 1 Merchant for its own credit card billing, AT&T is familiar with, subject to, and currently validated for the Payment Card Industry Data Security Standard (PCI DSS) requirements. The PCI DSS is generally inapplicable to telecommunication service providers (i.e., transport-only suppliers). However, an industry-recognized Qualified Security Assessor (QSA) for PCI validated AT&T to enable its customers to meet their PCI obligations. So, AT&T adheres to PCI standards.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	SSAE-16 SOC2 TYPE2 Report
AT&T Cloud Web Security Service	IaaS	Yes	SSAE16, ISO27001
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Services adheres to security standards that match or exceed the best practices outlined by: • The Center for Internet Security • AT&T Labs • AT&T Security Policy Requirements (ASPR), • Cisco Security. Also, effective June 15, 2011, the SAS 70 was replaced by the domestic US Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). The formal audit report under the new standard is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1". The SOC 3 Report, also known as a SysTrust Report, covers the following principles—Application Services: Security, Availability and Processing Integrity; Enterprise Hosting: Security and Availability. This report is made publically available for distribution. PCI:

AT&T Product	Category	Comply (yes/no)	AT&T Response
			As a certified Level 1 Merchant for its own credit card billing, AT&T is familiar with, subject to, and currently validated for the Payment Card Industry Data Security Standard (PCI DSS) requirements. The PCI DSS is generally inapplicable to telecommunication service providers (i.e., transport-only suppliers). However, an industry-recognized Qualified Security Assessor (QSA) for PCI validated AT&T to enable its customers to meet their PCI obligations. So, AT&T adheres to PCI standards.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact provides assertions around these infrastructures • PCI AOC (self attestation for all clusters, QSA for C14) • SOC 2 Type II • Safe Harbor • CPNI • ECPA As a public corporation, inContact abides by Sarbanes Oxley with SOX 404 testing.
AT&T Premises-Based Firewall Service	IaaS	See Comment	SAS-70 SOC II, SSAE 16/ISAE 3402, ISO 27001, PCI Compliant
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	SAS-70 SOC II, SSAE 16/ISAE 3402, ISO 27001, PCI Compliant
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	PCI, ISO, FISMA,BITS, HIPAA, FedRAMP, NIST 800-53, NIST 800-171, FIPS 200

8.6.3 Offeror must describe 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.

AT&T Response:

AT&T uses a wide range of security policies and procedures to protect its data centers from external threats.

These policies and procedures protect all aspects of our data center environments, including networks, databases, applications, and sensitive client information.

We use a variety of services, practices, and actions to provide this protection, including

- N+ Architecture—We employ an N+ architecture, a proven redundancy technique for mitigating risk throughout our networks. We protect uninterruptible power sources (UPSs) and other essential power sources at N+2 and chillers at N+1. This redundancy allows us to always have additional systems available.
- Multiple firewalls—Our networks include multiple firewalls that filter unwanted traffic and allow access to only necessary services.
- Multiple authentication methods—We use multiple authentication methods to verify information sources, including Virtual Private Network (VPN) authentication, application authentication, and secure shell authentication.
- Proactive security monitoring—We provide continuous, proactive security monitoring and reporting services to detect breaches in security.
- Dedicated client service—We provide one or more dedicated servers for each client. Therefore, you receive increased network security because your data and applications aren't on shared servers.
- Security reviews—We perform scheduled security reviews and audits to verify the performance and operation of all security measures.
- Isolated private VLAN—We provide isolated private Virtual Local Area Networks (VLANs) that separate network traffic from server to server and client to client.
- Traffic security—We use VPNs to encrypt network traffic and direct it to specific servers.

As a result, we can provide a secure and reliable environment for your critical data and applications.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T uses a wide range of security policies and procedures to protect its data centers from external threats. These policies and procedures protect all aspects of our data center environments, including networks, databases, applications, and sensitive client information. We use a variety of services, practices, and actions to provide this protection, including: • N+ Architecture—We employ an N+ architecture, a proven redundancy technique for mitigating risk throughout our networks. We protect uninterruptible power sources (UPSs) and other essential power sources at N+2 and chillers at N+1. This redundancy allows us to always have additional systems available. • Multiple firewalls—Our networks include multiple firewalls that filter unwanted traffic and allow access to only necessary services. • Multiple authentication methods—We use multiple authentication methods to verify information sources, including Virtual Private Network (VPN) authentication, application authentication, and secure shell authentication. • • Proactive security monitoring—We provide continuous, proactive security monitoring and reporting services to detect breaches in security. • Dedicated client service— UC Services are supported in a virtualized environment with all UC customers assigned to separate volumes within this virtualized environment. All customers are deployed on unique separate VLANS tied to customer VRFs. As such, UC Customers are logically separated from each other and no one customer can access another customer's logical calling space or data stores. • Security reviews—We perform scheduled security reviews and audits to verify the performance and operation of all security measures. • Isolated private VLAN—We provide isolated private Virtual Local Area Networks (VLANs) that separate network traffic from server to server and client to client. • Traffic security—We use VPNs to encrypt network traffic and direct it to specific servers. As a result, we can provide a secure and reliable

AT&T Product	Category	Comply (yes/no)	AT&T Response
			environment for your critical data and applications.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans employs a wide range of security management practices to provide a secure and reliable service to our customers. This includes network firewalls throughout the infrastructure to create security zones for different applications and services. Blue Jeans also deploys proxy servers that terminate all third-party / customer traffic at a proxy layer. Statefull firewalls (L2-4) and router/switches (L2-3) are deployed throughout the infrastructure to create separate security zones for different applications and services. All web traffic is run through an industry leading load balancer that protects against a suite of application attack vectors. Routers, firewalls, load balancers, and proxy application servers are all configured to mitigate numerous types of DOS attacks. Beyond the firewall, proxy servers and load balancers, Blue Jeans also periodically scans for network, port, and application-level vulnerabilities. Furthermore, all of the third-party applications and operating system software is checked for security advisories and is patched periodically. Blue Jeans periodically engages third-party consultants to perform a penetration test of the service (this is performed at least quarterly). We also leverage tools that do weekly scans in our data centers. As a standard, Blue Jeans restricts access to the production environment to only those employees with a job function(s) that requires access. As part of our SSAE 16 SOC 2 compliance, we get regularly audited to confirm our security controls align.
AT&T Cloud Web Security Service	IaaS	Yes	All AT&T Cloud Web Security Service points of presence are protected by hardware security stacks to help ensure protection from exterior threats. Additionally all network operations center personnel are put through strict screening processes in addition to the role based administration rules that govern their actions.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T uses a wide range of security policies and procedures to protect its data centers from external threats. These policies and procedures protect all aspects of our data center environments, including networks, databases, applications, and sensitive client information. The DDoS Scrubbers sit in N+1

AT&T Product	Category	Comply (yes/no)	AT&T Response
			datacenters with HA configurations and SOC2 controls.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T uses a wide range of security policies and procedures to protect its data centers from external threats. These policies and procedures protect all aspects of our data center environments, including networks, databases, applications, and sensitive client information. We use a variety of services, practices, and actions to provide this protection, including: • N+ Architecture—We employ an N+ architecture, a proven redundancy technique for mitigating risk throughout our networks. We protect uninterruptible power sources (UPSs) and other essential power sources at N+2 and chillers at N+1. This redundancy allows us to always have additional systems available. • Multiple firewalls—Our networks include multiple firewalls that filter unwanted traffic and allow access to only necessary services. • Multiple authentication methods—We use multiple authentication methods to verify information sources, including Virtual Private Network (VPN) authentication, application authentication, and secure shell authentication. • Proactive security monitoring—We provide continuous, proactive security monitoring and reporting services to detect breaches in security. • Dedicated client service— UC Services are supported in a virtualized environment with all UC customers assigned to separate volumes within this virtualized environment. All customers are deployed on unique separate VLANS tied to customer VRFs. As such, UC Customers are logically separated from each other and no one customer can access another customer's logical calling space or data stores. • Security reviews—We perform scheduled security reviews and audits to verify the performance and operation of all security measures. • Isolated private VLAN—We provide isolated private Virtual Local Area Networks (VLANs) that separate network traffic from server to server and client to client. • Traffic security—We use VPNs to encrypt network traffic and direct it to specific servers. As

AT&T Product	Category	Comply (yes/no)	AT&T Response
			a result, we can provide a secure and reliable environment for your critical data and applications.
AT&T Hosted Contact Center Service	SaaS	N/A	Our network switches and inContact application server centers are housed at secured, class-5 or 7, carrier-grade facilities in Los Angeles and Dallas. These are secure facilities; the servers are locked in secured data equipment cabinetry and the facility is monitored remotely at the inContact NOC center and by remote site personnel. Dallas security features include: • Multi-layer security control procedures • Key cards • 24 x 7 closed-circuit video and alarm monitoring • Uninterruptible redundant AC and DC power solutions that are flexible and upgradeable — meeting all types of customer needs • HVAC-redundant design with air distribution under raised flooring for maximum temperature control • Smoke detection systems above and below raised flooring • Double-interlock, pre-action, dry-pipe fire suppression LA security features includes: • State-of-the-art fire life safety system in place including a pre-action riser to the 30th floor. • All tenant fire life safety systems are tied to the base building fire life safety system which is supported by an automatic transfer switch to one of the building's standby power generators. • All common areas are sprinklered. • 24-hour attended lobby and security staff with integrated CCTV and card access systems. • Perimeter and sensitive areas monitored 24/7 from Security Station located on Ground Floor. • Elevators are security card controlled to prevent unauthorized use. • inContact offices are security card controlled with closed circuit cameras on the doors to control entry to the facility. The inContact solution uses multi-tenant architecture. inContact customers are assigned a “Business Unit” which no other inContact customer can access. Each

AT&T Product	Category	Comply (yes/no)	AT&T Response
			"Business Unit" is self-contained and allows for all contracted functionality.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to this service as no customer applications or data reside in the environment utilized to manage the service. For a description of the methodologies used to secure AT&T service delivery environments please see the Webex description three products above.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to this service as no customer applications or data reside in the environment utilized to manage the service. For a description of the methodologies used to secure AT&T service delivery environments please see the Webex description three products above.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Threats outside the data center are mitigated either by our Kona Site Defender or Prolexic products. Kona Site Defender stops web applications attacks near the source of the malicious activity. Kona Site Defenders intercepts threats at the edge of the internet, near the attacker keeping malicious threats away from your origin. Prolexic mitigate DDoS attacks by diverting the user traffic to a closest scrubbing center where mitigation is applied. For threats within the data center, ACDN follows the guidelines specified by FedRAMP, PCI, HIPAA etc.

8.6.4 Offeror must describe 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).

AT&T Response:

AT&T information security policy describes the various classifications of data, including customer information, and the associated protections that are mandated according to the environments in which it is transmitted and/or stored. Sensitive customer information is accorded at least the same protections as sensitive AT&T information.

In addition, our employees receive security training, sign confidentiality agreements upon employment, and annually acknowledge their responsibilities regarding protection of customer information.

See table below for additional product-specific commentary.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T information security policy describes the various classifications of data, including customer information, and the associated protections that are mandated according to the environments in which it is transmitted and/or stored. Sensitive customer information is accorded at least the same protections as sensitive AT&T information. In addition, our employees receive security training, sign confidentiality agreements upon employment, and annually acknowledge their responsibilities regarding protection of customer information
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a multi-tenant service. No client data is stored within the service aside from basic user account information (user name, password (SHA256 salted hash), profile picture when provided, email address. Other non-required information when provided and meeting recordings if the optional feature is enabled. Additionally call detail metadata is also stored and used for billing purposes as well as service performance and enhancement measures. All databases are in the US. Audio, Video and content sharing is not saved or stored on the Blue Jeans Cloud unless the meeting is recorded (optional). Recording can be disabled per user or the entire organization. Meeting chat is available during the meeting and it's not stored; this feature can also be disabled per user or for the entire organization as well. There is no file sharing capability with the service, user can show their screens during the meeting but there no native file sharing. Blue Jeans complies with US-EU Safe Harbor in order to comply with European privacy laws. US-EU & US-Swiss Safe Harbor Programs: We participate in the US-EU & US-Swiss Safe Harbor Frameworks covering the collection, use and retention of personal information gathered in the European Union member countries and Switzerland. Our participation means that we self-certify that we adhere to the Safe Harbor principles of notice, choice, onward transfer, security, integrity,

AT&T Product	Category	Comply (yes/no)	AT&T Response
			access and enforcement with respect to such personal information. To learn more about the Safe Harbor program, and to view our certification page, please visit: http://www.export.gov/safeharbor/ https://bluejeans.com/privacy-policy, http://bluejeans.com/site/acceptable-use-policy Blue Jeans Network Security Features Guide
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service's ISO27001 and SSAE16 certifications confirm that these processes are in place. Full reports can be provided upon request.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T uses ISO 27001 control standards and SOC2 controls to protect and verify the confidentiality of Customer data.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T information security policy describes the various classifications of data, including customer information, and the associated protections that are mandated according to the environments in which it is transmitted and/or stored. Sensitive customer information is accorded at least the same protections as sensitive AT&T information. In addition, our employees receive security training, sign confidentiality agreements upon employment, and annually acknowledge their responsibilities regarding protection of customer information.
AT&T Hosted Contact Center Service	SaaS	Yes	All client connections use HTTPS with TLS encryption and X.509 certificates. Secure FTP sessions use SSL Ver 3, AES 256. All access to the inContact platform and applications is security permission and role based. The security profiles restrict access to applicable roles and functions, as well as provides an audit history on any changes to platform inContact maintains a Trust Office with responsibility to assure that the business operations includes best practices for detection, threat protection, and policy violation, and to scan and test for vulnerabilities.
AT&T Premises-Based Firewall Service	IaaS	See Comment	AT&T information security policy describes the various classifications of data, including customer information, and the associated protections that are mandated according to the environments in which it is transmitted and/or stored. Sensitive customer information is accorded at least the same protections

AT&T Product	Category	Comply (yes/no)	AT&T Response
			as sensitive AT&T information. In addition, our employees receive security training, sign confidentiality agreements upon employment, and annually acknowledge their responsibilities regarding protection of customer information.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	AT&T information security policy describes the various classifications of data, including customer information, and the associated protections that are mandated according to the environments in which it is transmitted and/or stored. Sensitive customer information is accorded at least the same protections as sensitive AT&T information. In addition, our employees receive security training, sign confidentiality agreements upon employment, and annually acknowledge their responsibilities regarding protection of customer information.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN adheres to the FedRAMP standard of data confidentiality.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's security policies align with International Standards Organization ISO 27001:2005 standards. In 2011, we obtained certification of our compliance with this standard. See the following link for our ISO 27001 certificate and statement of applicability: • http://cso.att.com/ISO27001/index.html This means that we've successfully demonstrated our security controls to a third-party auditor. Also, Effective June 15, 2011, the SAS 70 was replaced by the

AT&T Product	Category	Comply (yes/no)	AT&T Response
			domestic US Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). The formal audit report under the new standard is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1". The SOC 3 Report, also known as a SysTrust Report, covers the following principles—Application Services: Security, Availability and Processing Integrity; Enterprise Hosting: Security and Availability. This report is made publically available for distribution.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	SSAE-16 SOC2 TYPE2 Report
AT&T Cloud Web Security Service	IaaS	Yes	SSAE16, ISO27001, FedRamp is being investigated
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Noted. AT&T will respond to this line item.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T's security policies align with International Standards Organization ISO 27001:2005 standards. In 2011, we obtained certification of our compliance with this standard. See the following link for our ISO 27001 certificate and statement of applicability: • http://cso.att.com/ISO27001/index.html This means that we've successfully demonstrated our security controls to a third-party auditor. Also, Effective June 15, 2011, the SAS 70 was replaced by the domestic US Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). The formal audit report under the new standard is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1". The SOC 3 Report, also known as a SysTrust Report, covers the following principles—Application Services: Security, Availability and Processing Integrity; Enterprise Hosting: Security and Availability. This report is made publically available for distribution.
AT&T Hosted	SaaS	Yes	Certifications include: SAS70 audited data centers, PCI

AT&T Product	Category	Comply (yes/no)	AT&T Response
Contact Center Service			compliance, Safe Harbor certification, change control policies, regular and timely security patch management, disaster recovery planning and security training provide regulatory compliance and service integrity. Our dedicated Trust Office actively participates in the Cloud Security Alliance (CSA). Note: It is inContact's position that pursuing FISMA is not appropriate. That said, we are looking to undergo a project to become FedRAMP compliant which are the federal security standards for cloud service providers. FedRAMP is a spinoff of FISMA.
AT&T Premises-Based Firewall Service	IaaS	Yes	SAS-70 SOC II, SSAE 16/ISAE 3402, ISO 27001, PCI Compliant,
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	SAS-70 SOC II, SSAE 16/ISAE 3402, ISO 27001, PCI Compliant
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Please refer to the Akamai FedRAMP link: https://www.fedramp.gov/marketplace/compliant-systems/akamai-content-delivery-services/

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This reusable framework minimizes the cost, time, and staff required to conduct redundant agency security assessments.

FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DOD), the National Security Agency (NSA), the Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

The FedRAMP requirements include additional controls above the standard NIST baseline controls in NIST SP 800-53 rev4 for low and moderate systems. These additional controls address the unique elements of cloud computing to help ensure that all federal data is secure in cloud environments.

FedRAMP provides a unified, government-wide risk management framework that increases agency confidence in cloud systems security.

The framework focuses on three areas:

- Providing joint security assessments and authorizations based on a standardized baseline set of security controls
- Using approved Third Party Assessment Organizations (3PAOs) to consistently evaluate a Cloud Service Provider's (CSP's) ability to meet the security controls
- Coordinating continuous monitoring services

The following link provides more detail about our FedRAMP compliance:

- https://www.fedramp.gov/marketplace/compliant-systems/att-storage-as-a-service-iaas/

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.

AT&T Response:

We log all users who access customer premises devices, and we flag and block users with repeated failed login attempts. To comply with AT&T's internal password standards, we change passwords regularly. And we review passwords when we reassign or terminate an employee.

The result is that your customer premises network equipment is secure.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T UC Services supports monitoring of all accesses and changes to its managed environment and to maintain logs for auditing purposes. • User ID • Role of the user • Number of login attempts • Modifications that were made, by whom, and when, for each administration session AT&T UC Services Support Center maintain three levels of troubleshooting logs as follows: • Info and Error – a log of system-level events • Functional Log – information to trace sessions

AT&T Product	Category	Comply (yes/no)	AT&T Response
			through the system, such as an audit trail, including the MACDs • Event Log – more detailed event information than a functional log about a process or service. End-user IT administrators have access to system logs that indicate changes to their information, profile, preferences, or configuration. Similar to logs described above, the audit trail contains the date and time stamp, the items that were changed, and the login ID of the person who made the changes.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Audit logs are running continuously so that access to all infrastructure components are constantly monitored. We leverage home grown auditing tools that can set event and or audit criteria based on preventive, corrective, and detective control. We currently log all activities on our jump-box server. Logs are currently stored indefinitely. All production and non-production logs from the Blue Jeans video conferencing application for addressing performance issues including call detail records, call debugging information, and application authentication logs are stored in centralized log/statistics reporting engine. In addition, system security logs from the infrastructure are also logged. System and User level login are enabled to help ensure proper detective level diagnostics. We have a log management tool to aggregate all logs to maintain the health of the service. Logs are kept indefinitely. All Blue Jeans components utilized various logging techniques ranging from proprietary, SLTF, MLTF, and Syslog formats. All logs are sent to a centrally managed server for alerting and archiving capabilities.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service logs all web browsing transactions within the service. Additionally all user access and configuration changes within the cloud portal management interface are logged. Web browsing transaction logging can be disabled, or limited to specific data utilizing the service's log anonymization capabilities.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	As part of the greater SIEM managed by AT&T, log files for Customer DDoS Service instances are logged and fed into the correlation engine of the SIEM.
AT&T Unified Communications as	SaaS	Yes	AT&T UC Services supports monitoring of all accesses and changes to its managed environment and to

AT&T Product	Category	Comply (yes/no)	AT&T Response
a Service			maintain logs for auditing purposes. • User ID • Role of the user • Number of login attempts • Modifications that were made, by whom, and when, for each administration session AT&T UC Services Support Center maintain three levels of troubleshooting logs as follows: • Info and Error – a log of system-level events • Functional Log – information to trace sessions through the system, such as an audit trail, including the MACDs • Event Log – more detailed event information than a functional log about a process or service. End-user IT administrators have access to system logs that indicate changes to their information, profile, preferences, or configuration. Similar to logs described above, the audit trail contains the date and time stamp, the items that were changed, and the login ID of the person who made the changes.
AT&T Hosted Contact Center Service	SaaS	Yes	The infrastructure logs and events are currently reviewed as needed by inContact staff. Since inContact uses the SaaS model, the customer does not have access to the infrastructure, so no customer access is provided for the infrastructure logs. Infrastructure monitoring (real time) is provided by the inContact NOC (Network Operations Center). Application logs are accessible for many of the inContact applications (like Central). Customers view the logs using Administrator ID access. Monitoring is provided using the inContact Central real time reporting tool.
AT&T Premises-Based Firewall Service	IaaS	Yes	The premise based firewall will generate syslog files that AT&T monitors for activity related to the security policy on the device. These are transmitted via an IPSEC tunnel to the security operations center for central logging, monitoring, and reporting.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	The premise based IDS/IPS device will generate syslog files that AT&T monitors for activity related to the security policy on the device. These are transmitted via an IPSEC tunnel to the security operations center for central logging, monitoring, and reporting.
AT&T Professional	IaaS	N/A	

AT&T Product	Category	Comply (yes/no)	AT&T Response
Services			
AT&T Content Delivery Network Service	IaaS	Yes	ACDN supports logging in CLF, W3C or hybrid of the two formats. Logs are collected at 15-30 minute intervals and can be transferred to the customer's local SIEM.

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

AT&T Response:

AT&T limits, controls, monitors, and audits third-party access to its customers' systems via authentication and approval management tools.

Our authenticating server verifies users and their credentials so that only the personnel responsible for managing customer networks have access.

We also do the following:

- Log all access attempts to customer-premises devices
- Flag repeated failed login attempts
- Block offending accounts

At regular intervals, we also change router passwords, which must comply with AT&T's internal password policies. When strong authentication is necessary, we require two-factor, token-based authentication to access a customer’s managed elements.

This means that we access customers’ systems only when necessary.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T limits, controls, monitors, and audits third-party access to its customers' systems via authentication and approval management tools. Our authenticating server verifies users and their credentials so that only the personnel responsible for managing customer networks have access. We also do the following: • Log all access attempts to customer-premises

AT&T Product	Category	Comply (yes/no)	AT&T Response
			devices • Flag repeated failed login attempts • Block offending accounts At regular intervals, we also change router passwords, which must comply with AT&T's internal password policies. When strong authentication is necessary, we require two-factor, token-based authentication to access a customer's managed elements. This means that we access customers' systems only when necessary.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a multi-tenant service, customer data is logically separated based on Enterprise IDs. These users have no account connection or access to other Enterprise organizations within Blue Jeans. No client data is stored within the service aside from basic user account information (user name, password (SHA256 salted hash), profile picture when provided, email address. Other non-required information when provided and meeting recordings if the optional feature is enabled. Additionally call detail metadata is also stored and used for billing purposes as well as service performance and enhancement measures. All databases are in the US. Blue Jeans primary database is stored on a fully redundant SAN infrastructure. The primary database is run with continuous replication to a secondary copy on an alternative mirrored SAN. The database is backed up periodically during the day to an offsite location. Database backups are logically write-protected when full backups are done. Routine testing is completed often to verify full fail over to DR sites.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Services uses role based administration which is followed by all Operations Center management chains.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Customer is granted access to the DDoS Service customer portal only after contracting for the service. Customer is responsible for all sub-accounts established in their portal.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T limits, controls, monitors, and audits third-party access to its customers' systems via authentication and approval management tools. Our authenticating server verifies users and their credentials so that only the personnel responsible for managing customer networks have access. We also do the following:

AT&T Product	Category	Comply (yes/no)	AT&T Response
			• Log all access attempts to customer-premises devices • Flag repeated failed login attempts • Block offending accounts At regular intervals, we also change router passwords, which must comply with AT&T's internal password policies. When strong authentication is necessary, we require two-factor, token-based authentication to access a customer's managed elements. This means that we access customers' systems only when necessary.
AT&T Hosted Contact Center Service	SaaS	Yes	All access to the inContact platform and applications is security permission and role based. The security profiles restrict access to applicable roles and functions
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to the managed firewall service but users that access the security portal are pre-authorized and limited to those given access for their roles.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to the managed IDS/IPS service but users that access the security portal are pre-authorized and limited to those given access for their roles.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	No data is hosted on the ACDN platform.

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.

AT&T Response:

AT&T does not monitor individual customer connections, except when they're part of a managed security service.

AT&T promptly notifies the customer of security incidents—via a customer care representative—when a detected intrusion attempt may affect the customer's service or information.

So, we make you aware of security incidents that may impact you.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T does not monitor individual customer connections, except when they're part of a managed security service. AT&T promptly notifies the customer of security incidents—via a customer care representative—when a detected intrusion attempt may affect the customer's service or information. So, we make you aware of security incidents that may impact you.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	In the event there is severe degradation or outage of the System, communication procedures are followed. If there is a suspected breach or known intrusion, the Security Incident and Reporting Process is triggered. The process begins when "notification" occurs or is initiated from an internal source or external customer source. All incidents are logged into the issue tracking and planning software application and tracked through to completion by Engineering/Support/IT/ NetOps teams. IT/NetOps will be responsible for performing an RCA (Root Cause Analysis) and communicating these incidents. NetOps and Security are responsible for communicating these incidents to the CTO and to log into the Company's private chat service to communicate specifics of an incident, status updates and continued posts for the duration of the incident. If the production environments are inaccessible for any significant period of time, Customer Support will notify affected customers and provide updates when the Blue Jeans service is restored. The incident response program has been tested and utilized from an availability perspective on a quarterly basis. Changes that impact system Security, Availability and Confidentiality are communicated to customers on the website prior to the change, maintenance or as a result of an outage/incident.
AT&T Cloud Web Security Service	IaaS	Yes	Low risk vulnerabilities are rarely communicated. However, high profile vulnerabilities are

AT&T Product	Category	Comply (yes/no)	AT&T Response
			communicated immediately (as soon as possible with intention to notify within 24 hours), alongside action plans for remediation.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS Service provides alerts and notifications based on mutually-agreed clipping levels established at activation. All notifications are provided only to those users identified in the customer portal.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T does not monitor individual customer connections, except when they're part of a managed security service. AT&T promptly notifies the customer of security incidents—via a customer care representative—when a detected intrusion attempt may affect the customer's service or information. So, we make you aware of security incidents that may impact you.
AT&T Hosted Contact Center Service	SaaS	Yes	We have a 24x7 on site NOC that monitors and gets alerted on various security signatures and incidents. When appropriate, these incidents will get escalated up to our network and systems engineering teams for further analysis. inContact does have policies and procedures that help ensure prompt notification of customers in the event of an incident, as well as procedures to address necessary remediation. Customer notification groups are configured and communications are sent out via email. Technical Account Managers also place phone calls out to the main contacts at our customers to alert of any security vulnerability, when identified.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to the managed firewall service as asked. Customer data is not held in this service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to the managed IDS/IPS service as asked. Customer data is not held in this service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	No data is hosted on the ACDN platform.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	UC Services are supported in a virtualized environment with all UC customers assigned to separate volumes within this virtualized environment. All customers are deployed on unique separate VLANS tied to customer VRFs. As such, UC Customers are logically separated from each other and no one customer can access another customer's logical calling space or data stores. Best practices for the deployment for VLAN infrastructure, including Switch and OS hardening is in accordance with The Center for Internet Security, AT&T Labs, AT&T Security Policy Requirements (ASPR), and Cisco Security, Cisco SAFE (Security Architecture For Enterprise).
AT&T Video Meetings with Blue Jeans	SaaS	Yes	All feature (or F) builds are part of the development process where the large, or boulder, issues are addressed. Subsequently, which features are targeting for release make it to "Master." Master is a branch in the code library which stores a superset code base of all of the software IP for the team and contains all code modules that will eventually make it to "Live" (production). A significant part of the quality testing is performed for the "Master" version of the code to ready it for promotion to the "Rel," another branch in the code library that includes the requisite code versions targeted for a specific release. After being tested in staging environment, the "Rel" version of the code is promoted up to "Beta," a new branch in the code library. The "Beta" version of the code is then tested in staging and receives approvals from the core Engineering, QA and Operations groups, and the "Beta" version of the code is first moved to production, or Z2 in Blue Jeans terminology, for limited release. This release allows an initial maturing process for release to customers as part of the beta process lasting approximately two or more weeks. If this limited release goes smoothly, the entire Blue

AT&T Product	Category	Comply (yes/no)	AT&T Response
			Jeans customer base on “Live” production, or Z1, will be updated.
AT&T Cloud Web Security Service	IaaS	Yes	All data centers used for hosting AT&T Cloud Web Security Service infrastructure are required to obtain or hold SSAE16, ISO27001, SOC1, SOC2, and SOC3 certifications. Additionally, cloud proxy hardware that is used to support the AT&T Cloud WSS is separated physically from all other hardware in each data center location.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS fully supports ZOCA architectures in its virtualized environments.
AT&T Unified Communications as a Service	SaaS	Yes	UC Services are supported in a virtualized environment with all UC customers assigned to separate volumes within this virtualized environment. All customers are deployed on unique separate VLANS tied to customer VRFs. As such, UC Customers are logically separated from each other and no one customer can access another customer’s logical calling space or data stores. Best practices for the deployment for VLAN infrastructure, including Switch and OS hardening is in accordance with The Center for Internet Security, AT&T Labs, AT&T Security Policy Requirements (ASPR), and Cisco Security, Cisco SAFE (Security Architecture For Enterprise).
AT&T Hosted Contact Center Service	SaaS	Yes	Your organization would have to further describe what you mean by ZOCA. We have a document which describes our topology, the inContact Technical FAQ, that indicates the configuration of edge routers, firewalls, gateways, and core switches that protect our surfaces. These are verified by our SOC 2 Type II and PCI AOC documents.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service because client servers are not hosted.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service because client servers are not hosted.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network	IaaS	N/A	No data is hosted on the ACDN platform.

AT&T Product	Category	Comply (yes/no)	AT&T Response
Service			

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)

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Reference architecture for AT&T Conferencing with Cisco WebEx service is proprietary to the AT&T service but can be reviewed on request.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans can supply a Network Overview and Security documentation upon request.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T can provide this on a case-by-case basis.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	Noted	AT&T can provide this on a case-by-case basis. Please refer to our response to Section 4, Business Profile, item 6.7
AT&T Unified Communications as a Service	SaaS	Yes	Reference architecture for the Unified Communication service is proprietary to the AT&T service but can be reviewed on request. In summary, AT&T uses a layered approach to security. Each layer builds upon the next to help ensure safeguards for our customers. AT&T UC Services adheres to security standards that match or exceed the best practices outlined by The Center for Internet Security, AT&T Labs, AT&T Security Policy Requirements (ASPR), and Cisco Security. AT&T also leverages a roles-based approach to the management and administration of the system. Managed environment infrastructure elements are compliant with AT&T Security Policy and Requirements (ASPR). ASPR will govern the creation of passwords and role-based access. Each user ID and password will be associated with a role that defines

AT&T Product	Category	Comply (yes/no)	AT&T Response
			and restricts which privileges or rights are available to that user. ASPR policy and associated role based privileges protects all access to communication channels and to data storage areas, including: access by end users, customer administrators, AT&T Customer Care, and AT&T Network Management. Each individual element must pass security vulnerability scans. A network element can only communicate directly with other network elements that are within the secure architecture—which means within a single company or organization.
AT&T Hosted Contact Center Service	SaaS	Yes	**POP Sites and Physical Security** Service integrity and security begin with the physical structure that house those services. inContact has two geographically diverse POP sites or data centers, housed in carrier grade facilities. These facilities were selected because of their ability to provide access to leading carriers and secure physical facilities. Coresite at One Wilshire, Los Angeles: • Described as one of the preeminent points for telecommunication and network • interconnection • 24x7 security using live guards and CCTV • Physical controls including man traps and card key access • Backup generators provide protected power • Only inContact employees have access to the inContact suite • In addition to building supplied backup generators all equipment is UPS and battery protected • Fully functional redundant cooling systems • Redundant and multiple fiber optic entrance facilities and Gig-E interfaces provide access to ISP's and telecom service providers Dallas – Level 3 Colocation facility: • Level 3 is one of the largest collocation providers in the world • 24x7 CCTV • Man traps and card key and biometric access controls • Fully protected power including backup generator • Climate control • inContact maintains separate locked equipment

AT&T Product	Category	Comply (yes/no)	AT&T Response
			cabinets within the facility • Redundant and multiple fiber optic entrance facilities and Gig-E interfaces provide access to ISP's and telecom service providers Telecom and Internet Network Architecture: • inContact connects to its service providers using redundant high capacity GigE and FastE interfaces as well as Time Division Multiplexed (TDM) services (DS1, DS3, OC3, OC12). TDM services utilize redundant fiber optic entrance facilities. • inContact uses conventional SS7 as well as the latest in VoIP SIP for rapid and reliable call set up. • inContact uses the top national carriers to provide diverse toll free (TF) routes and • Long distance termination routes. All telecom and Internet services are provisioned as redundant pairs or groups of services. • Services are designed to allow inContact to process TF and long distance calls using either Dallas or LAX POP sites. • inContact is a full service RESPORG, allowing us to route and reroute TF numbers between different carriers. This spreads traffic amongst multiple carriers and reduces risks and impact associated with the loss of a single carrier. • inContact utilizes two full service Lucent telecom switches to provide traditional long distance and dedicated services. These are fully redundant, fault tolerant systems. They are designed with redundant call processing and redundant TDM interface cards. Customers can create a redundant call design by installing multiple T1 or DS3 services, from one or both of the telecom switches. • The inContact telecom and Internet networks are designed to detect carrier and component failures and automatically redirect new voice and data traffic to redundant facilities
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN secure technical architecture fully complies with FedRAMP standard.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

AT&T Response:

AT&T provides the following information on the background checks we perform for our employees.

AT&T U.S.-Based Employee Background Check Policy

AT&T is committed to maintaining a workplace free of violence and to the protection of its employees, customers and assets. To promote consistency, the Company will conduct routine background checks on 100% of the finalists for employment positions within the U.S. It is AT&T's practice to conduct background checks that include foreign countries to the best of our ability and within our influence. We will respect the laws and customs of all foreign countries which may prohibit us from conducting a complete background check. In addition to conducting background checks on all new hires and rehires, AT&T also conducts background checks on current employees under the following circumstances:

- Employees moving into positions requiring checks not performed at the time of hire or into positions where checks are done on a scheduled basis.
- Employees moving into positions deemed to be highly sensitive, such as those having direct access to our network. Employees holding those positions are subject to additional background checks on a scheduled basis as deemed appropriate by the Business Unit.
- Employees directly supporting customers who have specific background check requirements built into their contract.
- Employees requiring access to a customer's secure location or to a facility shared with other companies.

- Checks of current employees against lists as required by state, local or Federal law.

Current employees who were not required to undergo a background check at the time of hire (including those acquired or insourced from other companies) will only be required to submit to a background check if they:

- support a customer for whom it is contractually required, or
- currently hold or are promoted or moved into a position requiring a complete or partial background check

Standard Background Check Elements for New Hire

The following elements are checked as standard procedure for applicable AT&T new hire employees.

- International Criminal -- All locations where an individual has lived, worked, or attended school for the past seven years if allowable by country law, using current name and any/all previous names/aliases provided.
- Federal Criminal Checks – Checks convictions in Federal jurisdictions of residence, education, and employment for the past seven years using current name and any/all previous names/aliases provided
- Nationwide Criminal Checks* – All felony and misdemeanor convictions for the past seven years, using current name and any/all previous names/aliases provided. All checks will be conducted using a nationwide criminal database in which most states participate.
- County Criminal Checks – All felony and misdemeanor convictions (charged and pending trial) in all counties of residence, education and employment for the past seven years using current name and any/all previous names/aliases provided
- Social Security Trace – Pulls history of all names and addresses associated with SSN
- Social Security Validation – Screens against the Death Master Index to validate that the SSN is legitimate and a valid number and does not belong to a deceased person. At a minimum it provides the approximate year of issuance.
- Motor Vehicle Records only for positions identified as regular driving positions, and Department of Transportation (D.O.T.) Records only for DOT positions. History will be based on state law, but generally a minimum of the past three years.

- Employment Verification – Confirms employment history provided by the candidate or employee, including Military history, for a minimum of five years.
- International Employment Checks when material to hiring decision or wage treatment (at discretion of Associate Director). All locations where an individual has lived, worked, or attended school for the past seven years if allowable by country law, using current name and any/all previous names/aliases provided.
- Previous AT&T Employment -- no limit in the period of time we check (new hires and acquisition)
- Education – (U.S.) Highest degree obtained (excluding GED/high school) when material to hiring decision or wage treatment (at discretion of Associate Director).
- International Education - Highest degree obtained (excluding GED/high school) when material to hiring decision or wage treatment (at discretion of Associate Director).
- Professional Licenses or Certifications - only those required for position or wage credit.
- U.S. Government Restricted Parties Checklists:
  - Specially Designated Nationals List: maintained by U.S. Department of the Treasury OFAC (Office of Foreign Asset Control) – database lists Specially Designated Nationals, including known terrorists: http://www.treasury.gov/offices/enforcement/ofac/sdn/index.shtml
  - List of Denied Parties maintained by the US Department of Commerce, Bureau of Industry and Security pursuant to the Export Administration Regulations (“EAR”) - lists persons and entities who have been denied export privileges for a certain period for violations of the EAR or other export laws: http://www.bis.doc.gov/dpl/Default.shtm
  - Entity List: maintained by the US Department of Commerce, Bureau of Industry and Security pursuant to the EAR - lists persons and entities deemed to pose a proliferation risk. http://www.bis.doc.gov/Entities/Default.htm
  - Unverified Parties List maintained by the US Department of Commerce, Bureau of Industry and Security pursuant to the EAR - lists foreign persons who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check or a post-shipment verification. Any transaction to an “Unverified” listed person does not automatically trigger a license requirement, but raises a “red flag” requiring further review. http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html

- State Department Nonproliferation Lists: Several lists compiled by the State Department of parties that have been sanctioned under various non-proliferation statutes. These are not maintained in one combined list, but can be accessed via the relevant underlying legislation or Executive Order, as applicable, through the following link: http://www.state.gov/t/isn/c15231.htm
- State Department's Debarred Parties List – lists parties debarred from participating directly or indirectly in the export of defense articles, including technical data or in the furnishing of defense services for which a license or approval is required by the International Traffic in Arms Regulations: http://www.pmddtc.state.gov/debar059.htm

- Credit Checks – Only as required by the customer contract or for specific positions (such as Officer positions).
- Sex Offender Registry Checks – National and all states individual lived, worked or attended school
- Federal Aviation Authority (FAA) Checks – Pilots only, if required for position.
- Media Checks – Officer positions only.
- Executive Affiliations- Officer positions only.

**Checks are conducted using a National Criminal Record Locator (NCRL) database. Information obtained from this source must be verified at the county level.*

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

AT&T Response:

AT&T's solution is implemented and operated in accordance with the security controls, guidelines, and standards, to the extent applicable, listed in the sections of Security Requirements and Information Use and Disclosure- Standards.

AT&T has a significant amount of demonstrated expertise and experience in the delivery of systems that are implemented and operated in accordance with FISMA, NIST SP 800-53, CJIS, and IRS 1075 security controls.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

AT&T Response:

The policies and procedures regarding notification vary according to the product and the nature, scope, and scale of the breach.

In the cases of major breaches directly impacting a given Purchasing Organization, AT&T will directly contact applicable Purchasing Organization contacts.

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.

AT&T Response:

AT&T understands. AT&T tracks the life cycle status for all in-scope assets. This includes end of support and end of life status and we provide you a semi-annual report. In addition, we perform annual audits to validate that the physical existence of assets and their corresponding detailed configurations are consistent with our configuration management database (CMDB).

If a network outage is scheduled, AT&T will use reasonable efforts to give you at least 30 days' notice before the planned maintenance.

If the network requires emergency maintenance, we'll provide you with as much advance notice as possible, depending on the urgency of the maintenance. However, we retain the authority to implement emergency maintenance at any time to help ensure a secure, healthy, and stable network environment.

As a result, you'll receive timely notification so that you can proactively work around scheduled or emergency outages.

Please refer to the table below for additional product-specific commentary.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T will work with the customer in good faith during the decommissioning process to help ensure services are maintained throughout the process, and the stated SLAs are met. Security of the customer data will be maintained as part of normal operations where stated AT&T procedures are followed that include need to know and assigned resources to the customer instance. Data can then be provided back to the customer by the AT&T Care team.
AT&T Video Meetings with Blue Jeans	SaaS	See Comment	Blue Jeans and AT&T renewal managers will notify the purchasing entity that they are up for service renewal. If the purchasing entity decides that they are not going forward with Blue Jeans, we would work with the IT admins to notify users to download recordings as needed. Users services will not be available after the access the service after the contract is expired and Blue Jeans will be able to work with IT admins from the purchasing entities to deprovision the user accounts.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is offered as a SaaS offering and since no data is retained in the cloud deprovisioning is simply removing customer access to the infrastructure. AT&T provides 12 months' notice prior to withdrawing or terminating a service and 120 days' notice prior to withdrawing or terminating a service component. AT&T Cloud Web Security Service only retains log files which customer has access to download from the customer portal at any time prior to the account deletion.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	At termination of the contract, AT&T will de-provision the BGP speaker, Access Router, and discontinue exporting customer flow data from the access router. At this point, the DDoS service ceases to function for the customer, and billing is discontinued.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T will work with the customer in good faith during the decommissioning process to help ensure services are maintained throughout the process, and the stated SLAs are met. Security of the customer data will be maintained as part of normal operations where stated AT&T procedures are followed that include need to know and assigned resources to the customer instance. Data can then be provided back to the customer in the form of the initial Audit Tool, self-

AT&T Product	Category	Comply (yes/no)	AT&T Response
			generated reports, and requested reports from the UC Voice Care team.
AT&T Hosted Contact Center Service	SaaS	Yes	If Purchasing Entity choose to terminate the contract before the contracted term then Purchasing Entity will pay the full contract value to the end of the agreed period. An exit plan is simply a written confirmation request that Purchasing Entity wishes to terminate the contract three months before the contract ends. Data Security is preserved during deprovisioning and transitioning as during the Service Term.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service because data is not transferred into or out of the service. Log information is available for download at service discontinuation of desired.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service because data is not transferred into or out of the service. Log information is available for download at service discontinuation of desired.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	AT&T gives enough notice (at least a year) before it marks a product as EOL. Customers of that particular product are sent regular and timely information related to EOL and transition plans. Account teams also work hand in hand with the customers to make this transition as smooth as possible.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Data can be provided back to the customer in the form of the initial bulk spreadsheet tool that the customer will have access to. In addition, the customer will have

AT&T Product	Category	Comply (yes/no)	AT&T Response
			access to a host list report in a 24-48 hour window.
AT&T Video Meetings with Blue Jeans	SaaS	See Comment	Blue Jeans does not own any data of the purchasing entity and the users will be able to download their recordings prior to the end of the service agreement.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service only retains log files which customer has access to download from the customer portal at any time prior to the account deletion.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	There is not data to return. When the service is discontinued, no data remains to be returned.
AT&T Unified Communications as a Service	SaaS	Yes	Data can be provided back to the customer in the form of the initial Site Audit Tool that the customer will have access to. In addition, the customer will have access to the VOSS administrator portal where data of the UC Voice instance will be available including location inventory, end station inventory, internal numbers, external numbers, analog lines, and other related information. Where information is not available in the two locations mentioned above; Site Audio Tool or VOSS, a variety of reports can be requested to be run and provided back to the customer in a normal MACD cycle.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact provides tools that allow customers to export data such as agents, or contact history. Relevant to that, it is entirely possible for a customer to perform their own data exporting. But should the customer desire assistance or need some form of special integration inContact has a Professional Services team that can assist (for a fee) in the extraction and migration of customer data to an alternate platform
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because no data is ingested.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because no data is ingested.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network	IaaS	N/A	No data is hosted on the ACDN platform.

AT&T Product	Category	Comply (yes/no)	AT&T Response
Service			

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. Experiences a business failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe outage.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Please see Attachment D for the AT&T Business Continuity Handbook.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	This is fully documented within the Blue Jeans SSAE-16 SOC2 TYPE2 Report. Blue Jeans has built a redundant network infrastructure to support our global cloud service. The service is hosted in multiple tier-4 co-location data centers around the world. We have a complete disaster recovery plan in place. This includes a full DR site via our US east coast data center. This should allow operational recovery in the event of a disaster within our targeted four-hour RTO (Recovery Time Objective). This is tested periodically and in our last test of this we were able to overachieve our target. The recovery objectives shall include: • Maintaining crucial business services for the

AT&T Product	Category	Comply (yes/no)	AT&T Response
			video collaborative solution. • Restoring operations to the primary production data center or designate a secondary (replacement) site to become the primary site. • Minimizing the loss of availability to the video conferencing service. • Testing (annually) and train for a disaster recovery with a scenario exercise. • Maximizing the resiliency capabilities by leveraging the contracted data hosting facilities. The recovery strategy shall encompass the critical components of the production databases beginning with backups through restoration and resumption of services. To help ensure backups are adequate, Blue Jeans Technical Operations have: • Created the ability to replicate between a multi master database cluster in the San Jose data center; • Exported and stored with an Enterprise grade Cloud Storage and Disaster Recovery Provider on a daily basis; and • Encrypted while stored at the Cloud Storage Provider. In the event of a defined incident, Blue Jeans will follow the incident response plan and help ensure the disaster recovery team executes a resolution during this real-world impacting event. Employees and industry standard tools provide continuous coverage to detect incidents and to manage the impact and provide resolutions in a timely manner. Key TechOps, Security personnel as well as Executive management members review this plan annually. Security, availability, data confidentiality and protection are the highest priorities for Blue Jeans. In an effort to raise the bar we're implementing a solution for data protection against complete site failure of our primary data center. While there are already mechanisms in place to protect against disk and node failures, Blue Jeans will extend this protection to site failure.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is offered as SaaS and is built on a highly available, fully meshed, load balanced infrastructure with fail over capability to eight Tier 1 connected US data centers. AT&T also provides 24x365 support via Helpdesk or web portal

AT&T Product	Category	Comply (yes/no)	AT&T Response
			with escalation paths as needed. AT&T works to meet Service Availability SLA objectives of 99.999%.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS scrubbers are geographically diverse as well as HA within an IDC.
AT&T Unified Communications as a Service	SaaS	Yes	Please see Attachment D for the AT&T Business Continuity Handbook.
AT&T Hosted Contact Center Service	SaaS	Yes	This is fully documented in our Standard Terms of Use and Support Level Agreement.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	See Comment	a) Extended downtime. The ACDN platform is designed to be self-healing. If one server cluster, data center or even network were to go down, traffic would automatically load balance to the fastest server cluster nearest to the off line one. With over 200,000 servers located in 94 countries peered with 1,000 networks, the ACDN platform is created out of an algorithm which mathematically routes around BGP and the Internet's outage. If a network or major Internet route were to suffer a fiber cut or other outage, we would route our customer's traffic. ACDN has never had a service outage on the entire platform. That is why we can offer a 100% availability SLA. b) Suffers an unrecoverable loss of data. ACDN pulls all data from the origin servers. Customers decide what to cache and what not. When an origin server suffers and outage, the customer may be able to leverage the data left in our cache to retrieve it. Note, ACDN does not provide origin hosting, but can act as a DR site for coverage c) Offeror experiences a system failure.

AT&T Product	Category	Comply (yes/no)	AT&T Response
			The ACDN platform is designed to be self-healing. If one server cluster, data center or even network were to go down, traffic would automatically load balance to the fastest server cluster nearest to the off line one. With over 200,000 servers located in 94 countries peered with 1,000 networks, the ACDN platform is created out of an algorithm which mathematically routes around BGP and the Internet's outage. If a network or major Internet route were to suffer a fiber cut or other outage, we would route our customer's traffic. ACDN has never had a service outage on the entire platform. That is why we can offer a 100% availability SLA. If a system failure ever were occurs, the Customer may elect to c-name its web site back to the origin infrastructure sending all traffic back. d) Ability to recover and restore data within four-business hours in the event of a severe system outage. ACDN does not provide origin hosting services. However, if the origin servers were to go down, ACDN can deliver a site from the last version in cache or provide a custom apology page. Multiple customers have benefitted from ACDN's ability to cache the static elements of a web site and deliver them rendering the vast majority of the web pages useful to the citizen while the RTO and RPO functions occur. e) Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO). ACDN offers a 100% availability SLA on the platform. The platform which consists of over 200,000 servers interconnected in 93 countries acts as a self-healing platform where if an outage occurred in one server cluster, data center or network, the traffic would automatically shift to the nearest or fastest ACDN cluster. The platform carries over 40 Million Hits per second and is designed to have 20% of its infrastructure off line for maintenance at any time. ACDN has not had an outage on the platform.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	UC Voice is hosted out of AT&T Internet Data Centers (IDCs) in the US.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	The database is backed up periodically during the day to an offsite location and stored in a fully encrypted manner for disaster recovery purposes. Database backups are encrypted while in transit and at rest. Data is encrypted in transit using at least 128bit AES over either IPSEC or SSL, or 2048 bit RSA when using asymmetrical encryption. As per our SSAE 16 SOC 2 report, restoration of database tests are completed on a regular basis to help ensure the integrity of backups. To help ensure production databases are recoverable, there is a replication process within the master database cluster in the San Jose data center. These database backups are also exported and stored with a designated third-party provider on a daily basis. For enhanced security, each database backup is encrypted in storage. The Blue Jeans service is a multi-tenant environment, internal backup logs are not available to customers. SOC 2 report shows evidence that backups are in place and control effectiveness over time. Report is available annually. Data is replicated between databases within the San Jose data-center and Virginia data center for DR capabilities, databases and code repositories are also backed up to Zetta on a nightly basis over HTTPS+SSL/SSH+rsync. Vendor risk assessments are conducted prior to conclusion of negotiations as well as on an annual basis. Risk assessments include Security questionnaires such as CCM or SIGv7, evaluation of vendor SOC2 controls and examination of ISO27001 certifications if applicable. In the case of Zetta, a security questionnaire and evaluation of their SOC2 report were conducted and are described in our own SOC2 report.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Cloud Web Security Service	IaaS	Yes	The AT&T Cloud Web Security Service is fully meshed and redundant, both within data centers and across data centers. Under that principle, data backups, server image backups, and other disaster recovery related backups are constant, and immediately dispersed throughout the cloud infrastructure.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	UC Voice is hosted at two AT&T Internet Data Centers (IDCs) in the US. One is located in the Dallas, TX, metro area and the other is in the Boston, MA, metro area.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact is a hosted platform with duplicated points of presence in Los Angeles, CA and Dallas, TX. Each of these clusters maintains real-time backups of the other. Restoration from secondary to primary occurs in minutes and there is no disruption of active sessions or sessions in queue during this process. No calls or sessions are lost to the inContact application.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	No data is hosted on the ACDN platform.

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.

AT&T Response:

AT&T uses industry-standard encryption techniques and algorithms. Generally, and where local law permits, we use standard encryption techniques, including

- Advanced Encryption Standard (AES) (128 and 256)
- Triple Data Encryption Standard (3DES)
- Commercial algorithms, including RC4 with a minimum equivalent of 128 bit

The specific algorithm depends on the application and the encryption mechanism, such as Secure Socket Layer (SSL), Secure Shell (SSH), Internet Protocol Security (IPSec).

AT&T's information security policy fully documents encryption requirements without necessarily prescribing specific products to use. In the few cases where a corporate standard product may be unavailable, business units use products that meet customer needs and the needs of the business. In addition, the use of any encryption algorithm or device must comply with all applicable local and in-country laws and regulations.

So, we use encryption to protect data from compromise.

Data at Rest

AT&T encrypts your data at rest according to your requirements.

We use Public Key Infrastructure (PKI) technology to encrypt data at rest. To create and authorize your certificates, we work with the PKI vendor that you prefer.

This means that we secure your data to meet your conditions.

Data in Motion

AT&T encrypts your data at rest according to your requirements.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	WebEx meeting password protection available for each meeting, optional user-selectable and controlled via Outlook scheduling Audio bridge password (PIN) can be optionally applied by the meeting/bridge host Unique PIN assigned to participants data

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Video Meetings with Blue Jeans	SaaS	Yes	The database is backed up periodically during the day to an offsite location and stored in a fully encrypted manner for disaster recovery purposes. Database backups are encrypted while in transit and at rest. Data is encrypted in transit using at least 128bit AES over either IPSEC or SSL, or 2048 bit RSA when using asymmetrical encryption. As per our SSAE 16 SOC 2 report, restoration of database tests are completed on a regular basis to help ensure the integrity of backups. To help ensure production databases are recoverable, there is a replication process within the master database cluster in the San Jose data center. These database backups are also exported and stored with a designated third-party provider on a daily basis. For enhanced security, each database backup is encrypted in storage. The Blue Jeans service is a multi-tenant environment, internal backup logs are not available to customers. SOC 2 report shows evidence that backups are in place and control effectiveness over time. Report is available annually. Data is replicated between databases within the San Jose data-center and Virginia data center for DR capabilities, databases and code repositories are also backed up to Zetta on a nightly basis over HTTPS+SSL/SSH+rsync. Vendor risk assessments are conducted prior to conclusion of negotiations as well as on an annual basis. Risk assessments include Security questionnaires such as CCM or SIGv7, evaluation of vendor SOC2 controls and examination of ISO27001 certifications if applicable. In the case of Zetta, a security questionnaire and evaluation of their SOC2 report were conducted and are described in our own SOC2 report.
AT&T Cloud Web Security Service	IaaS	Yes	All traffic between the customer and AT&T Cloud Web Security Service is encrypted in transit, while the options for long term encryption storage is available if necessary.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS scrubbers only process IP requests and filter them according to customer rules sets. No data is stored.
AT&T Unified Communications as	SaaS	Yes	AT&T uses industry-standard encryption techniques and algorithms. Generally, and where local law

AT&T Product	Category	Comply (yes/no)	AT&T Response
a Service			permits, we use standard encryption techniques, including • Advanced Encryption Standard (AES) (128 and 256) • Triple Data Encryption Standard (3DES) • Commercial algorithms, including RC4 with a minimum equivalent of 128 bit The specific algorithm depends on the application and the encryption mechanism, such as Secure Socket Layer (SSL), Secure Shell (SSH), Internet Protocol Security (IPSec). AT&T's information security policy fully documents encryption requirements without necessarily prescribing specific products to use. In the few cases where a corporate standard product may be unavailable, business units use products that meet customer needs and the needs of the business. In addition, the use of any encryption algorithm or device must comply with all applicable local and in-country laws and regulations. So, we use encryption to protect data from compromise. Data at Rest: AT&T encrypts your data at rest according to your requirements. We use Public Key Infrastructure (PKI) technology to encrypt data at rest. To create and authorize your certificates, we work with the PKI vendor that you prefer. This means that we secure your data to meet your conditions. Data in Motion: AT&T encrypts your data at rest according to your requirements. We use Public Key Infrastructure (PKI) technology to encrypt data at rest. To create and authorize your certificates, we work with the PKI vendor that you prefer. This means that we secure your data to meet your conditions.
AT&T Hosted Contact Center Service	SaaS	Yes	Data transport uses encryption in transit with strong encryption and public X.509 certs, etc. Optionally per contract, data can be encrypted while at rest at our EFT (Enhanced File Transfer) terminal. Customer provides their own keys.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Log data sent from the premise device to the security operations center is encrypted via an IPSEC tunnel.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Log data sent from the premise device to the security operations center is encrypted via an IPSEC tunnel.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

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.

AT&T Response:

AT&T is willing to comply with this requirement dependent upon the specifics of the applicable Business Associate Agreement and requirements of the Purchasing Entity.

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.

AT&T Response:

AT&T adheres to all applicable federal, state, and local laws. In addition, AT&T proposes the following response regarding Confidential Information:

Confidential Information

Confidential Information

Confidential Information means: (a) information the parties or their Affiliates share with each other in connection with an Agreement or in anticipation of providing Services under an Agreement (including pricing or other proposals), but only to the extent identified as Confidential Information in writing; and (b) except as may be required by applicable law or regulation, the terms of an Agreement.

Obligations

A disclosing party's Confidential Information will, for a period of three years following its disclosure to the other party (except in the case of software, for which the period is indefinite): (a) not be disclosed, except to the receiving party's employees, agents, and contractors having a need-to-know (but only if such agents and contractors are not direct competitors of the other party and agree in writing to use and disclosure restrictions as restrictive as this Section) or to the extent authorized to be revealed by law, governmental authority, or legal process (but only if such disclosure is limited to that which is so authorized and prompt notice is provided to the disclosing party to the extent practicable and not prohibited by law, governmental authority or legal process); (b) be held in confidence; and (c) be used only for purposes of using the Services, evaluating proposals for new services or performing an Agreement (including in the case of AT&T to detect fraud, to check quality and to operate, maintain and enhance the network and Services).

Exceptions

The restrictions in this Section will not apply to any information that: (a) is independently developed by the receiving party without use of the disclosing party's Confidential Information; (b) is lawfully received by the receiving party free of any obligation to keep it confidential; or (c) becomes generally available to the public other than by breach of this Agreement.

Privacy

Each party is responsible for complying with the privacy laws applicable to its business. AT&T shall require its personnel, agents, and contractors around the world who process Customer Personal Data to protect Customer Personal Data in accordance with the data protection laws and regulations applicable to AT&T's business. If Customer does not want AT&T to comprehend Customer data to which it may have access in performing Services, Customer must encrypt such data so that it will be unintelligible. Customer is responsible for obtaining consent from and giving notice to its Users, employees, and agents regarding Customer's and AT&T's collection and use of the User, employee or agent information in connection with a Service. Customer will only make accessible or provide Customer Personal Data to AT&T when it has the legal authority to do so. Unless otherwise directed by Customer in writing, if AT&T designates a dedicated account representative as Customer's primary contact with AT&T, Customer authorizes that representative to discuss and disclose Customer's customer proprietary network information to any employee or agent of Customer without a need for further authentication or authorization.

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.

AT&T Response:

The proposed products and services are designed to support a wide variety of state, local, federal, and commercial customers. Given such breadth, consistency across operations is of paramount importance. Custom SLAs imply exceptions to the standard processes, thus impacting consistency in service delivery. This tends to raise cost and hence price. Ironically, the incorporation of custom SLAs seldom results in reliability, availability, and performance gains that justify the additional cost.

The support model for all of the proposed services is predicated on a set of Service Level Objectives and/or Service Level Agreements, all of which are defined more fully in the applicable AT&T Service Guides in Attachment C.

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.

AT&T Response:

Please refer to the AT&T Service Guides in Attachment C for all SLA information.

8.11 (E) DATA DISPOSAL

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

AT&T Response:

AT&T's data erasure, destruction, and media disposal policy, as per our Information Classification and Protection Standard, mandates methods of data destruction and media sanitization according to media type and classification of information. We appropriately dispose of or sanitize paper and electronic media.

Our methods for disposing of electronic data include

- Overwrites
- Secure erase
- Degaussing
- Physical destruction of the media

So, we're committed to secure media disposal. Please refer to the table below for additional product-specific commentary.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's data erasure, destruction, and media disposal policy, as per our Information Classification and Protection Standard, mandates methods of data destruction and media sanitization according to media type and classification of information. We appropriately dispose of or sanitize paper and electronic media. Our methods for disposing of electronic data include • Overwrites • Secure erase • Degaussing • Physical destruction of the media So, we're committed to secure media disposal.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans utilizes an overwrite method using /dev/zero with a single pass for devices that will leave the organization that are functioning, storage devices that are not functioning when a system is retired are removed from the device and stored until they can be properly destroyed. Blue Jeans helps ensure that storage media containing customer data is properly sanitized of all customer information in accordance with applicable laws and regulations prior to disposal or reuse for non-Blue Jeans processing.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Cloud Web Security Service	IaaS	Yes	Data deletion processes are automated - customer specific log file data is deleted no later than 60 days after account expiration and can be deleted manually upon request. Confirmations can be provided upon request, depending on the requirements of the customer.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	AT&T's data erasure, destruction, and media disposal policy, as per our Information Classification and Protection Standard, mandates methods of data destruction and media sanitization according to media type and classification of information. We appropriately dispose of or sanitize paper and electronic media. Our methods for disposing of electronic data include • Overwrites • Secure erase • Degaussing • Physical destruction of the media So, we're committed to secure media disposal.
AT&T Hosted Contact Center Service	SaaS	Yes	We have a documented Document Retention Policy. Data/documents retained/destroyed based on the retention period for each type of data/documents. The customer can specify data retention for call recordings.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to managed firewall service because no data is kept.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to managed IDS/IPS service because no data is kept.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

8.12 (E) PERFORMANCE MEASURES AND REPORTING

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.9%. Additional points will be awarded for 99.9% or greater availability.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Please refer to the Service Level Agreement within the Service Guides in Attachment C, which provide for a 99.9% uptime
AT&T Video Meetings with Blue Jeans	SaaS	Yes	January 2016 (uptime for prior 12 months, ending Jan 2016, was 99.95%). Blue Jeans has built a fully redundant network infrastructure to support the service globally. Each of the data-center locations has: • Dual redundant service provider-class L3 routers- Dual redundant firewalls- Dual redundant load balancers- L2 switches configured to mitigate single points of failure • Blue Jeans runs its own BGP routing sessions with three or more internet backbone providers in each location to provide redundancy in routing as well as route optimization to and from different networks. Blue Jeans has different components of the solution deployed in a distributed fashion across multiple nodes and across multiple data centers.
AT&T Cloud Web Security Service	IaaS	Yes	The performance objective for Service Availability for AT&T Cloud Web Security Service is that the Service is available 99.999% of the time and the configuration portal of the Service will be available 99.9% of the time, except as provided below. Please refer to the SLA section of the AT&T Service Guide – AT&T Cloud Web Security Service in Attachment C.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS Scrubbers are HA within an IDC and geographically diverse, providing more than 99.99% uptime.
AT&T Unified	SaaS	Yes	Please refer to the Service Level Agreement within

AT&T Product	Category	Comply (yes/no)	AT&T Response
Communications as a Service			the Service Guides in Attachment C, which provide for a 99.9% uptime
AT&T Hosted Contact Center Service	SaaS	Yes	inContact aggressively manages all trouble and performance events, to that point inContact contractually guarantees all inContact clients at least 99.99% uptime.
AT&T Premises-Based Firewall Service	IaaS	Yes	Service Level Target for single-availability service is 99.9%. For high-availability service (two premise firewall devices onsite) the service level objective is 99.999%
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Service Level Target for single-availability service is 99.9%. For high-availability service (two sensor devices onsite) the service level objective is 99.999%
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN provides 100% uptime/availability SLAs over the public internet.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Please refer to the Service Level Agreement within the Service Guides in Attachment C, which provide for a 99.9% uptime
AT&T Video Meetings with Blue Jeans	SaaS	Yes	January 2016 (uptime for prior 12 months, ending Jan 2016, was 99.95%)
AT&T Cloud Web Security Service	IaaS	Yes	The performance objective for Service Availability for AT&T Cloud Web Security Service is that the Service is available 99.999% of the time and the configuration portal of the Service will be available 99.9% of the

AT&T Product	Category	Comply (yes/no)	AT&T Response
			time, except as provided below. Please refer to the SLA section of the AT&T Service Guide – AT&T Cloud Web Security Service in Attachment C.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	SLAs pertinent to DDoS Defense are described in the Service Guide in Attachment C. (Section is SLA-5)
AT&T Unified Communications as a Service	SaaS	Yes	Please refer to the Service Level Agreement within the Service Guides in Attachment C, which provide for a 99.9% uptime
AT&T Hosted Contact Center Service	SaaS	Yes	inContact aggressively manages all trouble and performance events, to that point inContact contractually guarantees all inContact clients at least 99.99% uptime.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Service Level Target for single-availability service is 99.9%. For high-availability service (two premise firewall devices onsite) the service level objective is 99.999%
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Service Level Target for single-availability service is 99.9%. For high-availability service (two sensor devices onsite) the service level objective is 99.999%
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Please refer to Attachment C for the Service Guides including Service Level Agreements. We provide AT&T ACDN Standard Uptime Service and Related SLA criteria at the end of the attachment.

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.

AT&T Response:

The AT&T account support team includes a service management program to help ensure that we give you excellent support.

The participating entity will have access to our service management team for assistance with overseeing a project's implementation, maintenance, and billing phases.

In addition, we provide tools that allow you to efficiently interact with us for 24x7 support.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's Stewardship Program enables the Service Manager to access statistics on a monthly basis and proactively apply for the service level agreements (SLA) credits.
AT&T Video Meetings with Blue Jeans	SaaS	See Comment	In the event there is severe degradation or outage of the System, communication procedures are followed. If there is a suspected breach or known intrusion, the Security Incident and Reporting Process is triggered. The process begins when "notification" occurs or is initiated from an internal source or external customer source. All incidents are logged into the issue tracking and planning software application and tracked through to completion by Engineering/Support/IT/NetOps teams. IT/NetOps will be responsible for performing an RCA (Root Cause Analysis) and communicating these incidents. NetOps and Security are responsible for communicating these incidents to the CTO and to log into the Company's private chat service to communicate specifics of an incident, status updates and continued posts for the duration of the incident. If the production environments are inaccessible for any significant period of time, Customer Support will notify affected customers and provide updates when the Blue Jeans service is restored. The incident response program has been tested and utilized from an availability perspective on a quarterly basis. Changes that impact system Security, Availability and Confidentiality are communicated to customers on the website prior to the change, maintenance or as a result of an outage/incident.
AT&T Cloud Web Security Service	IaaS	Yes	Please refer to the SLA section of the AT&T Service Guide – AT&T Cloud Web Security Service in Attachment C for

AT&T Product	Category	Comply (yes/no)	AT&T Response
			SLA details. http://serviceguidenew.att.com/sg_CustomPreviewer?attachmentId=00P1A00000nZOwwUAG
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	SLAs pertinent to DDoS Defense are described in the Service Guide in Attachment C. (Section is SLA-5)
AT&T Unified Communications as a Service	SaaS	Yes	AT&T's Stewardship Program enables the Service Manager to access statistics on a monthly basis and proactively apply for the service level agreements (SLA) credits. We apply these credits directly to the account affected.
AT&T Hosted Contact Center Service	SaaS	Yes	Documented in our Standard Terms. Per our Terms: inContact commits to deliver 99.99% of uptime per month for service components of inContact Service, which are the services required for contact delivery. If inContact exceeds five (5) minutes (99.99% uptime) of downtime in any given month, Customer can request a credit which will be calculated and applied in accordance with Section 3 (Commitment Level) under General Software Terms above. Upon request inContact will issue a credit to Customer for inContact Service failures by components of service. Components of service consist of those specific service features included in and used by Customer with the service established under the Agreement, excluding inContact Long Distance and Local Loops. The inContact Platform service components are: • inContact ACD (the ability to deliver a contact) • inContact IVR (the ability to execute a script) • inContact agent or station login
AT&T Premises-Based Firewall Service	IaaS	See Comment	No service credits are provided for missed Service Level Targets.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	No service credits are provided for missed Service Level Targets.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN SLA Service Level Credit Calculation • Customer must submit a credit request to the AT&T Billing Dispute team (tel: 1-800-235-7524) within thirty (30) days of an Outage for an SLA credit.

AT&T Product	Category	Comply (yes/no)	AT&T Response
			• Unless otherwise defined for a specific SLA, below, "Outage" is defined as a continuous service interruption for a duration of 15 minutes or more. • The amount of SLA credit due to Customer is based upon the duration of the Outage applicable to the Service Component. • Customer will receive one, and only one, SLA credit (as its sole remedy) for the applicable Service Component for each 24 hour period during which one (1) or more Outages occur; each 24 hour period commences at the beginning of the initial Outage qualifying for the SLA credit. • SLA credit will be equal to one day's service charge attributed to the Service Component, calculated as a pro-rata amount of the applicable Minimum Monthly Commitment in Customer's Agreement. • The maximum number of SLA credits for a Service Component in any calendar month shall not exceed thirty (30). • AT&T shall consider the earlier of the following as the start time of the service interruption for purposes of SLA calculation: (i) the issuance of a downtime alert of the Service Component by the AT&T CDN monitoring systems; or (ii) Customer's notice to AT&T of the specified Outage. In each case, AT&T's monitoring technicians shall confirm the presence of an Outage. **ACDN Exception to SLA Credits** Customer shall not be entitled to SLA credits if an Outage is the result of: • Acts or omissions of Customer, Customer's Third Party vendors, or the end users accessing Customer's content. • Faults in the configuration of Customer Origin Servers, Websites or streams, (whether managed by Customer or outsourced) including but not limited to: publishing of non-existent URLs or URLs containing no information; failure to configure the AT&T CDN Service with a valid stream source; failure of Customer Origin Servers or the access to those servers; or addition of end user-specific arguments to a cacheable URL. • End user problems such as repeated abandonment of file download attempts, insufficient access speed, misconfiguration of end user client, and any other

AT&T Product	Category	Comply (yes/no)	AT&T Response
			end user issues not under the control of AT&T. • The performance of non-AT&T CDN Services, including but not limited to services provided to Customer by Third Parties or in association with other AT&T services. • Any failure that is not the fault of AT&T, its employees, its agents, its suppliers, or its representatives. • The failure of Customer to carry out any Customer obligations in the Agreement. • AT&T CDN Service volumes that exceed maximum information rate agreed to in Customer's Agreement. • Failure due to encoders and encoding formats and speeds not certified by AT&T. • Failure of code Managed and/or written by Customer or a Third Party vendor for Customer. • Customer managed application, encoder, or Customer Origin Server failures that disrupt or adversely impact service. • Customer preventing AT&T from implementing software patches or software upgrades that are necessary for AT&T to provide service commensurate with existing SLAs. • Customer's refusal to allow AT&T to perform maintenance that is deemed necessary to maintain service, whether scheduled or unscheduled. • Force Majeure Condition. • Measurement malfunctions (e.g., agent outage, agent network access, and other non-AT&T CDN root causes) **ACDN SLA Rules and Regulations** The following SLA rules and regulations are applicable to the service: • AT&T reserves the right to change or modify the SLA program rules and regulations at any time without notice, including but not limited to: o Amending or canceling any or all of the SLAs contained in this Service Guide o Implementing new SLAs o Implementing different measurement technologies or methodologies • Should any changes to the SLA program be

AT&T Product	Category	Comply (yes/no)	AT&T Response
			implemented, AT&T will amend this Service Guide as appropriate. • Only the Customer purchasing the service may make claims. There shall be no Third Party claimants or beneficiaries of the Service Level Agreements. • Customer must submit a credit request by calling the AT&T Billing Dispute team (tel: 1-800-235-7524) within 30 days from the time the SLA was not met. • Customer's sole remedy for AT&T's failures to meet the SLAs is service SLA credits as described in this service guide. • AT&T will be the sole party to determine whether an outage has occurred and that a failure to meet an SLA is worthy of an SLA credit.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

AT&T Response:

If a network outage is scheduled, AT&T will use reasonable efforts to give you at least 30 days' notice before the planned maintenance.

If the network requires emergency maintenance, we'll provide you with as much advance notice as possible, depending on the urgency of the maintenance. However, we retain the authority to implement emergency maintenance at any time to help ensure a secure, healthy, and stable network environment.

As a result, you'll receive timely notification so that you can proactively work around scheduled or emergency outages.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T will use reasonable efforts to give you at least 30 days' notice before the planned maintenance. If the network requires emergency maintenance, we'll provide you with as much advance notice as possible, depending on the urgency of the maintenance. However, we retain the authority to implement

AT&T Product	Category	Comply (yes/no)	AT&T Response
			emergency maintenance at any time to help ensure a secure, healthy, and stable network environment. As a result, you'll receive timely notification so that you can proactively work around scheduled or emergency outages.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Users will be notified via a banner when they login to their Blue Jeans account or when connecting to a Blue Jeans meeting. Planned maintenance periods are usually posted within 48 hours prior to the weekend maintenance. Our Customer Success Manager can also provide customize schedule maintenance windows messaging to enterprise users. We redirect users and provide the maintenance window information. Our planned maintenance outages are scheduled on weekends. By subscribing to the email updates on the service status page, users will receive an email message in case of a planned maintenance/outage periods. Just click on the Subscribe to updates option on the top-right corner and you can add as many email addresses/phone numbers you want to receive the notification via email/text message for planned/unplanned(outage) maintenance.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T will use commercially reasonable efforts to notify customers about larger service releases and data center maintenance at least two weeks in advance; and of all other maintenance releases at least seventy-two (72) hours in advance.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T will use commercially reasonable efforts to notify customers about larger service releases and data center maintenance at least two weeks in advance; and of all other maintenance releases at least seventy-two (72) hours in advance.
AT&T Unified Communications as a Service	SaaS	Yes	If a network outage is scheduled, AT&T will use reasonable efforts to give you at least 30 days' notice before the planned maintenance. If the network requires emergency maintenance, we'll provide you with as much advance notice as possible, depending on the urgency of the maintenance. However, we retain the authority to implement emergency maintenance at any time to help ensure a secure, healthy, and stable network environment. As a result, you'll receive timely notification so that you can proactively work around scheduled or emergency outages.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Hosted Contact Center Service	SaaS	Yes	The inContact application is continually updated via minor and major releases. Upgrades to our platform are always done during non-peak off hours. Our typical maintenance window is Friday from 12:00-3:00 AM (Mountain Time). The application platform is not taken off line in most cases, but if and when the platform is unavailable due to planned maintenance you will be given seven days' notice of such event.
AT&T Premises-Based Firewall Service	IaaS	Yes	AT&T may perform extensive maintenance up to four (4) times per year, and may also schedule planned maintenance. AT&T will use reasonable efforts to give Customer at least thirty (30) days prior notice (via email or other electronic means) of such scheduled or extended maintenance schedules. AT&T reserves the right to perform maintenance at any time in order to properly maintain the Service or AT&T's network. MSS is not designed to operate during scheduled maintenance (such as upgrade to Customer equipment, software, and capacity upgrades or the addition of new features).
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	AT&T may perform extensive maintenance up to four (4) times per year, and may also schedule planned maintenance. AT&T will use reasonable efforts to give Customer at least thirty (30) days prior notice (via email or other electronic means) of such scheduled or extended maintenance schedules. AT&T reserves the right to perform maintenance at any time in order to properly maintain the Service or AT&T's network. MSS is not designed to operate during scheduled maintenance (such as upgrade to Customer equipment, software, and capacity upgrades or the addition of new features).
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	The ACDN platform is 100% available.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's Stewardship Program enables the Service Manager to access statistics on a monthly basis and proactively apply for the service level agreements (SLA) credits.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	In the event of a defined incident, Blue Jeans will follow the incident response plan and help ensure the disaster recovery team executes a resolution during this real-world impacting event. Employees and industry standard tools provide continuous coverage to detect incidents and to manage the impact and provide resolutions in a timely manner. Key TechOps, Security personnel as well as Executive management members review this plan annually. Security, availability, data confidentiality and protection are the highest priorities for Blue Jeans. In an effort to raise the bar we're implementing a solution for data protection against complete site failure of our primary data center. While there are already mechanisms in place to protect against disk and node failures, Blue Jeans will extend this protection to site failure.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is offered as SaaS and is built on a highly available, fully meshed, load balanced infrastructure with fail over capability to eight Tier 1 connected US data centers. Please refer to the SLAs with the AT&T Service Guide - AT&T Cloud Web Security Service in Attachment C.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	SLAs pertinent to DDoS Defense are described in the Service Guides in Attachment C. (Section is SLA-5)
AT&T Unified Communications as a Service	SaaS	Yes	AT&T's Stewardship Program enables the Service Manager to access statistics on a monthly basis and proactively apply for the service level agreements (SLA) credits. We apply these credits directly to the account affected.
AT&T Hosted Contact Center Service	SaaS	Yes	In the event that SLAs are not met, customers can request service credits based upon the SLA matrix provided in the standard terms of use.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

AT&T Response:

AT&T provides a variety of reports. The content varies according to the product. Some reports are based on near real time data. Others are generated on a periodic "batch" basis. Further details are documented in the applicable Service Guides in Attachment C.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	A variety of reports can be provided by request from the UC Care Team, including usage reports, quality reports, etc.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans includes Command Center, which offers detailed stats including usage reports, quality, surveys, all real-time information. This includes the ability to filter based on various criteria such as meeting size and moderator. This tool is available via Web Portal login.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Administration portal also has robust reporting which includes usage, user, and threat reporting center allowing reports to be scheduled or produced in real time. These reports can be downloaded, e-mailed, and archived in PDF, CSV, and XML formats.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Please refer to Attachment C for the applicable Service Guide and additional information.
AT&T Unified Communications as a Service	SaaS	Yes	A variety of reports can be provided by requesting certain reports from the UC Care Team, or the customer can also be provided report access through the Cisco Administrative Reporting (CAR) tool to generate a wide variety or reporting capabilities that are specific to the customers UC instance, including Voice Transmission Quality report, Line Inventory Report, Specific Called Report, etc.
AT&T Hosted Contact Center Service	SaaS	Yes	Our reports are centralized in inContact Central. Reports are permissions-based, so only the reports the person is authorized to view are displayed. We have standardized reports, and reports that you can configure on-the-fly. We have a rich selection of real time, historical, standardized, and ad hoc options available. Since inContact Central is a browser-based client, they're available on any internet-connected computer.
AT&T Premises-Based Firewall Service	IaaS	No	SLA performance reports are not available but service related reports are available via the BusinessDirect Security Services portal. Report content consists of event and policy related data generated from "security related" devices managed and monitored by AT&T MSS (Managed Security Services). Reports summarize important Top 20 events MSS Report content is derived from device security logs and does not include system access, management or utilization data. AT&T MSS Security Best Practices and Customer-defined device logging procedures, may affect data that is ultimately displayed in MSS Reports. Report Data is updated on BusinessDirect daily and are available for each of the following levels • For each Asset (i.e. Sensor) • For each Site (Location) • For all Sites (Company level) Reports types are subject to change
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	No	SLA performance reports are not available but service related reports are available via the BusinessDirect Security Services portal. Report content consists of event and policy related data generated from "security related" devices managed and monitored by AT&T MSS

AT&T Product	Category	Comply (yes/no)	AT&T Response
			(Managed Security Services). Reports summarize important Top 20 events MSS Report content is derived from device security logs and does not include system access, management or utilization data. AT&T MSS Security Best Practices and Customer-defined device logging procedures, may affect data that is ultimately displayed in MSS Reports. Report Data is updated on BusinessDirect daily and are available for each of the following levels • For each Asset (i.e. Sensor) • For each Site (Location) • For all Sites (Company level) Reports types are subject to change
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	There are several ways to access performance reports: 1) Luna Control Center, our internet portal provides reports in two formats, HTML or CSV. 2) Configure reports to be automatically sent by email on a recurring basis in either HTML or CSV format. 3) Web Services using SOAP interface instead of a browser. 4) Luna Control Center MIB provides real time statistics and events directly to an end user's Enterprise Network Management System. SNMP MIDB download is available on Windows and Linus systems. 5) Log Delivery Service provides server logs for various services.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Conferencing with Cisco WebEx complies.
AT&T Video	SaaS	Yes	Blue Jeans includes Command Center, which offers

AT&T Product	Category	Comply (yes/no)	AT&T Response
Meetings with Blue Jeans			detailed stats including usage reports, quality, and surveys, all via real-time information. This includes the ability to filter based on various criteria such as meeting size and moderator.
AT&T Cloud Web Security Service	IaaS	Yes	Yes, AT&T Cloud Web Security complies.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Customer has access to historical reports via BusinessDirect.
AT&T Unified Communications as a Service	SaaS	Yes	A variety of reports can be provided by requesting certain reports from the UC Care Team, or the customer can also be provided report access through the Cisco Administrative Reporting (CAR) tool to generate a wide variety or reporting capabilities that are specific to the customers UC instance.
AT&T Hosted Contact Center Service	SaaS	Yes	Reports can be exported to Excel. Once in Excel, reports can be shared in a variety of ways, i.e., sent as an attachment to an email, printed, saved as .HTML, etc. All of the data in our reports can also be exported to other reporting tools as well in raw data formats.
AT&T Premises-Based Firewall Service	IaaS	Yes	Reports related to service delivery are available to print locally.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Reports related to service delivery are available to print locally.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Printing is available through the ACDN Luna Control Center.

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

AT&T Response:

Not all of the products proposed are engineered for "on demand" delivery. However, for those that are, services are designed for 24x7 availability, with the exception of

published maintenance windows. Further details are documented in the applicable Service Guides in Attachment C.

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

AT&T Response:

Not all of the products proposed are engineered for "scale-up/scale-down" delivery. However, for those that are, services are designed for 24x7 availability, with the exception of published maintenance windows. Further details are documented in the applicable Service Guides in Attachment C.

8.13 (E) CLOUD SECURITY ALLIANCE QUESTIONNAIRES

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

a. Completion of a CSA Star Self-Assessment, as described in Section 5.5.3.

b. Completion of Exhibits 1 and 2 to Attachment B.

c. Completion of a CSA Star Attestation, Certification, or Assessment.

d. Completion CSA Star Continuous Monitoring.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Beyond its own stringent internal procedures, the WebEx Office of Security engages multiple independent third parties to conduct rigorous audits against internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. These auditors include Information Security Partners, LLC (iSEC Partners) for exhaustive network routing

AT&T Product	Category	Comply (yes/no)	AT&T Response
			and application, and PriceWaterhouseCoopers, for SAS-70 Type II attestation, including auditing of controls against ISO 17799 controls. **iSEC Network Routing** iSEC Partners completed a variety of tests to confirm the routing to and from WebEx Meeting Attendees and the WebEx Collaboration Cloud. The tests covered both traces for WebEx production servers, and route confirmation traces for various network device configurations that included routers, firewalls, and load balancers. The results of this testing indicate that communication for U.S.-based WebEx sites does not route outside of the U.S. For more information, you may request a copy of this report from the WebEx Office of Security. **iSEC Source Code Review** iSEC Partners performs ongoing, in-depth code-assisted penetration tests and service assessments. During these engagements, iSEC Partners receives access to WebEx servers, source code, and engineering staff. Unlike black box testing, this high degree of access enables iSEC Partners to: • Identify critical application and/or service vulnerabilities and propose solutions. • Recommend general areas for architectural improvement. • Identify coding errors and provide guidance on coding practice improvements. • Work directly with WebEx engineering staff to explain findings and provide guidance for remediation work. For more information, you may request a copy of this report from the WebEx Office of Security **SAS-70 Type II** PricewaterhouseCoopers LLP performs an annual SAS-70 Type II audit in accordance with standards established by the AICPA. The controls audited against WebEx are based on ISO-17799 standards. This highly respected and recognized audit validates that WebEx services have been audited in-depth against control objectives and control activities (that often include controls over information technology and security related processes) with respect to handling and processing customer data. For additional information on the SAS-70 standard please

AT&T Product	Category	Comply (yes/no)	AT&T Response
			see: www.sas70.com/index2.htm. For more information, you may request a copy of PricewaterhouseCoopers LLP SAS-70 report from the WebEx Office of Security via your Cisco account representative. **ISO-17799** ISO-17799 is an internationally recognized information security standard published by the International Organization of Standardization (ISO) that provides best practice recommendations on information security management. It defines requirements for corporate security policies, data management, and access control, among other things. PricewaterhouseCoopers LLP compared WebEx security policies and practices to the control objectives described in ISO-17799, second edition for Information Technology - Security Techniques. The result of the audit was positive. In the opinion of PricewaterhouseCoopers WebEx services provide adequate controls as defined in this standard. For additional information on the ISO-17799 standard please see: www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm **Conclusion** Your organization can trust WebEx to enable collaboration and streamline business processes—in even the most stringent security environments. Choose easy to use, reliable, proven, and secure Software-as-a-Service collaboration solutions from AT&T.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans carries a SSAE-16 SOC 2 Type II compliance which is a key component of CSA Level 2 Attestation certification. We can share this report under Unilateral NDA.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service has completed a STAR self-assessment; however, level 2 CSA STAR Registry assessments and attestations have not been completed. Please see our completed CAIQ in Attachment B.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	We currently do not test against Star Registry. We are a founding member of the CSA, where we pay annual dues and have representation on committees.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Services adheres to security standards that match or exceed the best practices outlined by: • The Center for Internet Security • AT&T Labs • AT&T Security Policy Requirements (ASPR), • Cisco Security. Also, effective June 15, 2011, the SAS 70 was replaced by the domestic US Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). The formal audit report under the new standard is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1". The SOC 3 Report, also known as a SysTrust Report, covers the following principles—Application Services: Security, Availability and Processing Integrity; Enterprise Hosting: Security and Availability. This report is made publically available for distribution. PCI: As a certified Level 1 Merchant for its own credit card billing, AT&T is familiar with, subject to, and currently validated for the Payment Card Industry Data Security Standard (PCI DSS) requirements. The PCI DSS is generally inapplicable to telecommunication service providers (i.e., transport-only suppliers). However, an industry-recognized Qualified Security Assessor (QSA) for PCI validated AT&T to enable its customers to meet their PCI obligations. So, AT&T adheres to PCI standards.
AT&T Hosted Contact Center Service	SaaS	See Comment	We currently do not test against Star Registry. We are a founding member of the CSA, where we pay annual dues and have representation on committees. We do fill out responses to both the CSA-CCM and CAIQ 3.1. If those documents may be helpful, please request them through your designated sales person.
AT&T Premises-Based Firewall Service	IaaS	No	AT&T Premises-Based Firewall is a managed service which is not related to the series of questions that make up the CSA STAR registry. This is simply due to the form and function of the devices and services provided. Since they are not related to data manipulation or storage, processing or orchestration the STAR assessment is not applicable. Data centers and facilities utilized to deliver the service are strictly controlled via various certification efforts as identified previously.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	No	AT&T Intrusion Detection/Prevention is a managed service which is not related to the series of questions that make up the CSA STAR registry. This is simply due to the form and function of the devices and services provided. Since they are not related to data manipulation or storage, processing or orchestration the STAR assessment is not applicable. Data centers and facilities utilized to deliver the service are strictly controlled via various certification efforts as identified previously.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	No	Please refer to the completed CAIQ Questionnaire in Attachment B for additional information

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T provides the ability for the customer to make changes at a user level through the 24x7 customer care center. This means that emergency changes at that level can happen real-time.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans has a formal implementation plan that is being fine-tuned with every Purchasing Entity. The ongoing contact around implementations is arranged between the Customer Success team at Blue Jeans and the Purchasing Entity. It is important to mention that almost all ongoing changes will be able to be addressed by the Administrator for Blue Jeans at the Purchasing Entity. That person(s) is empowered to

AT&T Product	Category	Comply (yes/no)	AT&T Response
			make most of the necessary ongoing changes to their Blue Jeans environment. Other tasks can be fulfilled by sending a request to our support department or our customer success manager for the Purchasing Entity. With their 24x7 availability we can assure that at any time your request can be received and an implementation timeframe can be defined for you.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is offered as SaaS which the infrastructure is prebuilt allowing AT&T the ability to respond to customer expeditious needs as required.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	AT&T provides, for a fee, an expedited installation of DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T provides the ability for the customer to make changes at a user level through the administrative portal on a 24x7 basis. This means that emergency changes at that level can happen real-time. Customers can also choose to contact the UC Care team directly where tickets can be submitted and fulfilled through that team. Larger scale changes will be required to be worked through the account team who will have the customer's best interest understood and will assist in escalating emergency requests.
AT&T Hosted Contact Center Service	SaaS	Yes	Current customers have access to our "Professional Services on demand" program where PS services can be purchased in 15 minute increments, for making emergency call flow/call handling changes to existing customers. New, first time "emergency" turn up or new implementations can be accommodated upon request, with specific and defined pricing provided prior to each engagement.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Managed security services deployment milestones have both AT&T and client responsibilities that affect timeline. Depending on applicable hardware availability and client provided information service deployment may be accelerated.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Managed security services deployment milestones have both AT&T and client responsibilities that affect timeline. Depending on applicable hardware availability and client provided information service deployment may be accelerated.
AT&T Professional	IaaS	N/A	

AT&T Product	Category	Comply (yes/no)	AT&T Response
Services			
AT&T Content Delivery Network Service	IaaS	Yes	An Emergency Integration fee is assessed when a customer requires an ACDN service integrated on a faster than normal timeline (less than 10 business days) The Purchasing Entity will contact AT&T Sales/ Professional Services Team to initiate emergency request.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Estimated time for provisioning is 30 to 45 days
AT&T Video Meetings with Blue Jeans	SaaS	Yes	After an order has been placed from a customer and the order was submitted by AT&T. Blue Jeans provisioning is standard lead-time is 24-48 hrs.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T complies with requirements 8.4.2 - Once order is accepted service can be provisioned in 48 hours.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Standard lead-time for DDoS service is 14-21 business days following acceptance of a fully executed Agreement.
AT&T Unified Communications as a Service	SaaS	Yes	90 days is the estimated delivery timeframe for AT&T's Unified Communications service
AT&T Hosted Contact Center Service	SaaS	See Comment	The lead time for processing a new, first time deployment ranges from 30 to 90 days, depending on the complexity, agent count/training requirements, and features being implemented. A detailed project plan will be provided prior to any deployment project outlining responsibilities by party involved, along with expected completion time. Every deployment will be overseen by a project manager, experienced in the deployment of the inContact solution.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Premises-Based Firewall Service	IaaS	See Comment	Service is typically designed, deployed, tested, and operational between forty-five and sixty days from signed contract.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Service is typically designed, deployed, tested, and operational between forty-five and sixty days from signed contract.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	The standard lead time for integration on to the ACDN platform is typically 10-15 business days depending on customer availability, number of services ordered and complexity of solution.

8.15 (E) BACK UP AND DISASTER PLAN

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Webex is a multi-tenant service. No client data is stored within the service aside from basic user account information (user name, password (SHA256 salted hash), profile picture when provided, email address. Other non-required information when provided and meeting recordings if the optional feature is enabled. Additionally call detail metadata is also stored and used for billing purposes as well as service performance and enhancement measures. All databases are in the US.,
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a multi-tenant service. No client data is stored within the service aside from basic user account information (user name, password (SHA256 salted hash), profile picture when provided, email

AT&T Product	Category	Comply (yes/no)	AT&T Response
			address. Other non-required information when provided and meeting recordings if the optional feature is enabled. Additionally call detail metadata is also stored and used for billing purposes as well as service performance and enhancement measures. All databases are in the US. Audio, Video and content sharing is not saved or stored on the Blue Jeans Cloud unless the meeting is recorded (optional). Recording can be disabled per user or the entire organization. Meeting chat is available during the meeting and it's not stored; this feature can also be disabled per user or for the entire organization as well. There is no file sharing capability with the service, user can show their screens during the meeting but there no native file sharing. Blue Jeans complies with US-EU Safe Harbor in order to comply with European privacy laws. US-EU and US-Swiss Safe Harbor Programs: We participate in the US-EU and US-Swiss Safe Harbor Frameworks covering the collection, use and retention of personal information gathered in the European Union member countries and Switzerland. Our participation means that we self-certify that we adhere to the Safe Harbor principles of notice, choice, onward transfer, security, integrity, access and enforcement with respect to such personal information.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security keeps one year of live log files and three years of raw log files.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	Limited customer data is stored with that being in the form of UC system account detail and voicemail messaging. The account detail is retained with active or suspended accounts, and the messaging retention is at the discretion of the end users or administrators who have ultimate control over the saving or deleting of those messages. All other data is transitionary and not applicable.
AT&T Hosted Contact Center Service	SaaS	Yes	AT&T Hosted Contact Center Service offers the ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.
AT&T Premises-	IaaS	No	Not applicable because data is not stored within

AT&T Product	Category	Comply (yes/no)	AT&T Response
Based Firewall Service			managed firewall service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	No	Not applicable because data is not stored within managed IDS/IPS service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	ACDN does not store customer's data. In the event of an outage, our caches are restored from the customer's origin website.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T has disaster recovery mechanisms in place today and has redundancy built in at the data center and cross data center levels. The Data Centers can operate in a fail over mode to take over from another data center at any time. Software versions are hardened to avoid any risk of intrusions or virus threats. The DCs have dual optical fiber connections into each location and have power fail over procedures in place. Also access to the DCs is strictly limited according to SOC Type 2
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans has disaster recovery mechanisms in place today and has redundancy built in at the data center and cross data center levels. The Data Centers can operate in a fail over mode to take over from another data center at any time. Software versions are hardened to avoid any risk of intrusions or virus threats. The DCs have dual optical fiber connections into each location and have power fail over procedures in place. Also access to the DCs is strictly

AT&T Product	Category	Comply (yes/no)	AT&T Response
			limited according to SOC Type 2 as well as ISO 27001 certifications.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is offered as SaaS and is built on a highly available, fully meshed, load balanced infrastructure with fail over capability to eight Tier 1 connected US data centers.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T has disaster recovery mechanisms in place today and has redundancy built in at the data center and cross data center levels. The Data Centers can operate in a fail over mode to take over from another data center at any time. Software versions are hardened to avoid any risk of intrusions or virus threats. The DCs have dual optical fiber connections into each location and have power fail over procedures in place. Also access to the DCs is strictly limited according to SOC Type 2
AT&T Hosted Contact Center Service	SaaS	Yes	Our customers rely on inContact when emergency situations arise that could impact their ability to answer calls. Since inContact is a cloud-based solution, with redundancy built in, you are automatically provided with a disaster recovery or business continuity option to continue operations. inContact maintains a redundancy level for inContact that includes, but not limited to, servers, power systems, communications ports, data bases, and other key components. If one element suffers a failure, the level of redundancy affords that, through load sharing, a customer does not have all of their critical components (ports, data storage devices, etc.) located on a single device, but spread over several devices to minimize the effect of a service outage of a single component. The system is distributed and mirrored across multiple sites. Many inContact customers have worked with inContact to develop emergency notification processes. These processes notify them when queuing becomes excessive, no agents are signed in, when database issues arise, etc. This notification can be done electronically (email) or via the phone. When an emergency arises the plan can be put into action automatically.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Premises-Based Firewall Service	IaaS	See Comment	AT&T invests heavily in technology, processes and people to help ensure our services are available. To illustrate our commitment, in March, 2012, the Department of Homeland Security (DHS) announced that AT&T became the first company to be certified to DHS's Voluntary Private Sector Preparedness Program (PS-Prep). PS-Prep™ is a partnership between DHS and the private sector enabling private entities to receive Business Continuity certification. The PS-Prep™ program recognizes private sector organizations that enhance their capabilities for planning, responding to, and recovering from events and other threats.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	AT&T invests heavily in technology, processes and people to help ensure our services are available. To illustrate our commitment, in March, 2012, the Department of Homeland Security (DHS) announced that AT&T became the first company to be certified to DHS's Voluntary Private Sector Preparedness Program (PS-Prep). PS-Prep™ is a partnership between DHS and the private sector enabling private entities to receive Business Continuity certification. The PS-Prep™ program recognizes private sector organizations that enhance their capabilities for planning, responding to, and recovering from events and other threats.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T has disaster recovery mechanisms in place today and has redundancy built in at the data center and cross data center levels. The Data Centers can operate in a fail over mode to take over from another data center at any time. Software versions are hardened to avoid any risk of intrusions or virus threats. The DCs have dual optical fiber connections into each location and have power fail over procedures in place. Also access to the DCs is strictly limited according to SOC Type 2
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans has several Points of Presence (POPs) distributed globally. The voice and video media will be automatically directed to the closest POP to the endpoint or media egress point. Audio/ video traffic will be routed to any of our Tier 1 data centers in US, EU, Australia or Asia based on geographic location. Blue Jeans runs its own BGP routing sessions with 3 or more internet backbone providers in each location to provide redundancy in routing as well as route optimization to and from different networks. Blue Jeans has different components of the solution deployed in a distributed fashion across multiple nodes and across multiple data centers. From a capacity perspective we operate each data center at a capacity threshold. Once that capacity is being reached we upgrade the capacity with is easy due to the modular and virtualized buildup of the applications and hardware.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service is fully meshed and redundant, both within data centers and across data centers. Under that principle, data backups, server image backups, and other disaster recovery related backups are constant, and immediately dispersed throughout the cloud infrastructure.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	AT&T has disaster recovery mechanisms in place today and has redundancy built in at the data center and cross data center levels. The Data Centers can operate in a fail over mode to take over from another data center at any time. Software versions are hardened to avoid any risk of intrusions or virus threats. The DCs have dual optical fiber connections into each location

AT&T Product	Category	Comply (yes/no)	AT&T Response
			and have power fail over procedures in place. Also access to the DCs is strictly limited according to SOC Type 2
AT&T Hosted Contact Center Service	SaaS	Yes	Fully redundant and protected power is critical to today's data centers. With inContact, you receive carrier-grade service at a fraction of the cost. Our server centers operate with the most advanced equipment available to help ensure that you receive the best technology possible without having to purchase it on your own. inContact has four fully redundant cloud super-sites: two in North America (Dallas and Los Angeles) and two in Europe (Frankfurt and Munich). Our sites are supported and monitored by a 24/7 carrier-grade Network Operations Center (NOC) located at our corporate offices in Salt Lake City. The NOC employs next generation, industry-standard monitoring systems and tools and, in the event of failure, has the ability to operate remotely utilizing inContact technology either within Salt Lake City or Los Angeles. The inContact network is designed for redundancy and failover. The core IP network is connected via a dual SONET ring backbone, meaning two redundant fiber links. Along with redundant edge routers, core routers, firewalls and VoIP hardware, multiple ISP and diverse toll-free carriers, our network infrastructure provides reliable, stable, service-rich benefits. This broad range of connectivity models and solutions allows for the highest level of selection in hosted IP telephony and call center applications. Each server center functions as both a primary location, and as a backup to the other server center in the event of a problem. If a major outage were to take place in Dallas, for instance, the next call would be completed through the Los Angeles server center. All historical data, call flows and other information would continue uninterrupted. Our network operating centers function with 24/7 on-site securities. Through our IP backbone, our networking infrastructure connects our sites via bandwidth pipes that can be routed through a private connection. We also have state-of-the-art intrusion detection systems in place to keep our system safe

AT&T Product	Category	Comply (yes/no)	AT&T Response
			from hackers. inContact utilizes redundant equipment, facilities, connections, power supplies, cooling systems and databases to help ensure that your contact center is always up and running smoothly.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable as asked because a managed firewall service is not providing application services but be assured that business continuity is fully addressed in the delivering of our managed security services.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable as asked because a managed IDS/IPS service is not providing application services but be assured that business continuity is fully addressed in the delivering of our managed security services.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	See Comment	AT&T has combined Akamai's industry leading content delivery platform with AT&T's world-renowned IP network to deliver to NASPO members an exclusive suite of global CDN and telecom solutions. With the deployment of Akamai's CDN infrastructure within AT&T's network infrastructure, customers will benefit from more efficient content routing and better delivery of digital content, video, and Web applications. This results in a better end-user experience. AT&T has deployed Akamai CDN servers at the edge of its IP network and in AT&T facilities throughout the United States.

8.16 (E) SOLUTION ADMINISTRATION

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Customer is assigned a BusinessDirect account at service activation. They have full access to the account for as long as the service agreement is in effect. AT&T Webex Portal is also provided for users to make changes to their account.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	User management will be fully transferred to the Purchasing party. You have the option to start small with an import of users into the Blue Jeans environment in the cloud, where full administration of features and capabilities as well as security settings can be applied. Blue Jeans also uses the secure and widely adopted industry standard Security Assertion Markup Language (SAML), for Single Sign On method. This also means Blue Jeans implementation of SSO integrates easily with any large Identity Provider (IdP) that supports SAML. If you've built your own SAML--based federated authentication process, we integrate with that too. We support service-provider-initiated SAML and identity-provider-initiated SAML.
AT&T Cloud Web Security Service	IaaS	Yes	The AT&T Cloud Web Security Service administrative portal allows Customer administrators to view their corporate policies and manage the Service using a graphical, web-based interface. Once the customer administrator makes and saves changes to their policies and selects the Deploy button, the change is pushed to the Web Security gateway, which is inspecting traffic. Management of users (add/delete users and user groups) will take place on the customer's Active Directory.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	Customer is assigned a BusinessDirect account at service activation. They have full access to the account for as long as the service agreement is in effect.
AT&T Unified Communications as a Service	SaaS	Yes	Customer is assigned an Admin account at service activation. They have full access to the account for as long as the service agreement is in effect. AT&T allows for discretionary administrative capability for users to locally make some changes to services once they are established users These include but are not limited to: • Voice mail options • User profile options • Adding voice users • Removing voice users • User levels of permissions/privileges

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Hosted Contact Center Service	SaaS	Yes	Every component of the inContact solution can be managed remotely since it is a cloud-based solution; however, Studio requires a download to a Windows-based computer. inContact Agent and Central are fully browser-based providing easy remote access. Central: A browser-based interface for handling such administrative tasks as viewing reporting, setting up user accounts, creating skill groups, assigning pre-recorded messages or music to specific events during the contact process. It is the "Central" administrative interface of the Product.
AT&T Premises-Based Firewall Service	IaaS	Yes	Access to AT&T Managed Security Services are limited to identified users during provisioning.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Access to AT&T Managed Security Services are limited to identified users during provisioning.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Managing users and roles can be performed through the ACDN Luna Control Center.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Anti-Virus is provided as part of the Webex Service. As a part of AT&T's Webex production architecture, we monitor for intrusions and look for the signatures of an intrusion. We also utilize enterprise grade anti-virus applications and apply Microsoft critical updates on a regular schedule
AT&T Video Meetings with Blue Jeans	SaaS	Yes	All Windows or OSX workstations provided by Blue Jeans will have Sophos Anti-Virus installed. The Blue Jeans service does not have typical file

AT&T Product	Category	Comply (yes/no)	AT&T Response
			upload/transfer services. Anti-virus and anti-malware software is installed on all workstations and corporate servers. Data-center systems run hardened OS with HIDS installed to prevent the installation and launching of malicious software. Linux systems in the datacenter utilize Centralized deployment management and file system and service integrity tools OSSEC to monitor for changes and access to systems that support the service. Host servers are running the latest Blue Jeans approved LINUX Ubuntu OS and Windows Server 2012. We run stripped down systems in our data-center and no software can be placed on the systems without our operations personnel intervention.
AT&T Cloud Web Security Service	IaaS	N/A	N/A - Using the AT&T Cloud Web Security Portal, the administrator can: • Manage Malware Scanning policies to control virus attacks, spam and spyware. • Allow administrators to view, create, change and delete Malware scanning profiles and file filter profiles
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service
AT&T Unified Communications as a Service	SaaS	Yes	As a part of AT&T's UC production architecture, we monitor for intrusions and look for the signatures of an intrusion. We also utilize enterprise grade anti-virus applications and apply Microsoft critical updates on a regular schedule
AT&T Hosted Contact Center Service	SaaS	Yes	As a part of inContact's production architecture, we monitor for intrusions and look for the signatures of an intrusion. We also utilize enterprise grade anti-virus applications and apply Microsoft critical updates on a regular schedule. All servers run Sophos antivirus applications. We utilize the IDS of the Palo Alto Firewalls.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because no data is ingested.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because no data is ingested.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	No data is hosted on the ACDN platform.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T provides System Administration training to Support Staff on the administration of the service prior to the system being transitioned. Live training and pre-recorded video tutorials can be accessed at any time An AT&T staff member will be assigned to assist in delivering training during the initial rollout period. These sessions are interactive and participants will be encouraged to ask questions and be part of the overall training experience. Training sessions will cover: call types, reservation instructions, helpful tips and techniques, teleconference feature descriptions, service contacts/support and teleconference applications. These meetings can include demonstrations, distribution of information, and question and answer sessions. AT&T encourages NASPO to take full advantage of the available service training and rollout for a variety of reasons. The education program will ultimately help NASPO by providing personalized service delivery to each business associate. In doing so, AT&T can help ensure a smooth roll as well as potential cost savings for NASPO by encouraging the end-user to use specific cost effective call types when applications do not warrant higher cost access methods. There are no fees or charges associated with the training sessions, and education is continually available. System administration training is provided and exact time will

AT&T Product	Category	Comply (yes/no)	AT&T Response
			be negotiated based upon current NASPO employee expertise.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	The Purchasing Entity remains is full control over all meta data as well as user data, which can be exported for the Purchasing Entity at any time. If the Purchasing Entity decides to use Single Sign On via an AD connection then all actual user information is at the Purchasing Entity.
AT&T Cloud Web Security Service	IaaS	N/A	There is no data to be migrated. AT&T Cloud Web Security Service provides network-based (cloud) web filtering, malware and content scanning of Customer-designated network users or devices, including roaming (not connected to Customer VPN) and mobile user support. AT&T is acting in its capacity as a data processor and will process the Traffic Data of Customer only on behalf of and under the direction of Customer (and its designees).
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	All telephony currently in service under contracts with the current contract provider (Legacy PBX Telephone Services and VoIP), including all legacy PBX ports and circuits and VoIP ports, shall be transitioned to the hosted VoIP. AT&T would work in close collaboration with the current contract provider to: • Identify all telephony targeted to be migrated • Perform all necessary technical assessments and planning needed for migration • Schedule migration by subset (location/department/floor, etc.) • Stage appropriate hard or soft phones, if applicable • Instruct the current contract provider to decommission/delete ports/seats once the migration is performed • Assume service, billing, maintenance and Help Desk support for migrated agents/ports/seats • Verify that all migrated ports/seats have been deleted from previous Contractors' billing at true-up.
AT&T Hosted Contact Center	SaaS	Yes	inContact has tools to export call data, call logs, agent data etc. from the cloud. The tools are designed to

AT&T Product	Category	Comply (yes/no)	AT&T Response
Service			facilitate the use of our system. We provide tools to export data for the purpose of using our service, not for the purpose of migrating to another system. inContact does not allow another data source to write directly into our database. However the data can be pulled in the methods described above into a third data source to combine the data sources together As a call contact management service, inContact only requires a minimum amount of data to operate, such as Agent name, Number, email and certain call performance metadata. Most our customers keep any PII data within their database architecture and does not reside within the inContact architecture. The data resides in the inContact cloud and is accessible by the customer, but controlled by inContact. The data specific to customer can be downloaded in a variety of formats
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because the service is not self-provisioned and no metadata is involved.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because the service is not self-provisioned and no metadata is involved.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN does not host origin content. All content is placed by the consumer of cloud services on what itself feels is cacheable in storage. As such, ACDN does not rely on origin infrastructure. In fact many clients switching from one cloud hosting provider to another leverage ACDN to make sure their static content remains up during a migration period. ACDN acts as a "swing site" for those migrating sites keeping the non-transactional elements operating smoothly during a live cutover from one cloud hosting to another. Moreover, as ACDN is a C Name change, a customer could easily turn ACDN off if it no longer wants the service without interruption. We would simply point them back to the origin for the content after the AT&T contract expired.

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

AT&T Response:

All of the products being proposed can be ordered by, and then delivered to, individual Purchasing Organizations.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	The AT&T Conferencing with Cisco WebEx Solution can be administered by the customer at an enterprise level or at a location level. Enterprise level access will have access to all customer locations in a hierarchical manner, and individual location administrators can be established where those administrators only have access to administer the users within that location. As a result, administration in a distributed manner can be accomplished.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	The Blue Jeans service will typically by administered via accessing the Web Portal. From there we have an Admin tab which not all users have access too. As the Blue Jeans admin you can select certain users to have access to the Admin tab for granular control. Users who have access to the admin tab can easily add/modify/remove all users, force password changes and password policies as well as many other items such as overall organization preferences.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security allows each participating entity their own administration portal and the ability to administer their own policies and users.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	The UC solution can be administered by the customer at an enterprise level or at a location level. Enterprise level access will have access to all customer locations in a hierarchical manner, and individual location administrators can be established where those administrators only have access to administer the users within that location. As a result, administration in a distributed manner can be accomplished, and the administrative portal is accessible over the Internet

AT&T Product	Category	Comply (yes/no)	AT&T Response
			with secure IDs and passwords so access is made available from a variety of locations.
AT&T Hosted Contact Center Service	SaaS	Yes	AT&T Hosted Contact Center Service allows each participating entity their own administration portal and the ability to administer their own policies and users.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because it's administered by each individual entity.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because it's administered by each individual entity.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN uses Content Provider Codes (CP) for tracking and reporting of delivered content. All CP Codes are tied to one or more service, which are then tracked and reported under that CP Code. The Luna Control Center Traffic, URLs, (Unique) Visitors, Response, Offload, etc. all display traffic information by CP code. CP Codes can be used to separate content or services for tracking and reporting purposes.

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

AT&T Response:

For those services allowing a "self-service" interface, Purchasing Organizations are free to implement their own administrative policies. For services associated with security (e.g., firewalls), AT&T will work with technical contacts within a given Purchasing Organization to fine-tune business and security rules and to establish a baseline of normal behavior. For those services with a more "one size fits all" delivery, fine-tuning administrative policy is not feasible.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T shall have MACD activity for the AT&T Conferencing with Cisco WebEx solution to include moves, additions, changes and deletion/removal of service. MACD services may also include a range of tasks including, but not limited to, minor software changes and project management for large site moves/installations/decommissioning.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	AT&T Video Meetings with Blue Jeans offers the ability to apply participating entity's defined administration polices in managing solution.
AT&T Cloud Web Security Service	IaaS	Yes	Each Purchasing Entity will have their own Administration Portal. The AT&T Cloud Web Security Service administrative portal allows Customer administrators to view their corporate policies and manage the Service using a graphical, web-based interface. Once the customer administrator makes and saves changes to their policies and selects the Deploy button, the change is pushed to the Web Security gateway, which is inspecting traffic. Management of users (add/delete users and user groups) will take place on the customer's Active Directory. • Using the portal, the administrator can: o Set web filtering policies (block and allow categories, white list/black list) o Block or allow predefined categories such as "Personal Relationships", "Internet Radio and TV", etc. which contain the most common URLs (facebook.com, myspace.com, pandora.com, etc.) o Block or allow predefined classifications such as "Image Search", "Video Search", etc. o Block or allow custom categories created by the customer administrator containing specific URLs defined by the customer administrator o Manage identity based user group policies- add, change, delete and move rules, o Manage Malware Scanning policies to control virus attacks, spam and spyware. o Allow administrators to view, create, change and delete Malware scanning profiles and file filter profiles. o Manage Application Control List Profiles for

AT&T Product	Category	Comply (yes/no)	AT&T Response
			IM, Audio and Video Streaming, etc. o Allow administrators to view, create, change and delete Application Control profiles and file filter profiles. o Manage Web Content Control policies to control Java applets, Active X and Cookies. • Allow administrators to view, create, change and delete Web Content Control profiles and file filter profiles.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	The service must use role-based access unique to each user. AT&T shall help ensure that these activities are secure and isolated to each user. These logins must include read-only and read-write administrative agents' permissions. AT&T shall have MACD activity for the hosted VoIP service to include moves, additions, changes and deletion/removal of service. MACD services may also include a range of tasks including, but not limited to, minor software changes and project management for large site moves/installations/decommissioning. AT&T shall have a secure web portal for in-take and processing of MACD requests. The portal must be available 24x7x365. The portal allows entry, edit, and view of all orders, order activity, order status, and order completion.
AT&T Hosted Contact Center Service	SaaS	Yes	The service uses role-based access unique to each user. AT&T will help ensure that these activities are secure and isolated to each user. These logins must include read-only and read-write administrative agents' permissions.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because it's administered by each individual entity.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because it's administered by each individual entity.
AT&T Professional Services	IaaS	N/A	

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Content Delivery Network Service	IaaS	Yes	The ACDN Luna Control Center offers customer self-service User Management capabilities. This tool allows customers and partners to create new users, define profiles and set access rights and privileges to deliver the right level of information, often matching the company's internal business structure.

8.17 (E) HOSTING AND PROVISIONING

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's Webex cloud is built in multiple data centers. No additional server requirements are needed. You purchase Webex on a license and audio basis.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Purchasing Entity Admins are able to provision accounts and do training for the provision process. Provisioning stack would be defined with each purchasing entity.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service offers 3 distinct products - Web Security, Hosted Reporting and Mobile Device Security. All products are offered only as a suite when sold with other AT&T products. As soon as a purchase order is received, that purchase order is processed, and all associated products are provisioned for access in the AT&T Cloud Web Security Service cloud infrastructure automatically.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T has built-out four AT&T UC PODS. No additional data center build is required. Individual customer provisioning takes 30-90 days.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Hosted Contact Center Service	SaaS	Yes	Please refer to Attachment C for the Service Guides.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not directly applicable because this is not a hosting service. However the deployment process for AT&T Premises-Based Firewall service is Step 1 – Data Collection Step 2 – Milestone Notification Step 3 – Preparing Your Environment Step 4 – Equipment Installation Step 5 - Test and Turn-up Step 6 – Transition Service(s) into Maintenance Step 7 – Service Completion Notice
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not directly applicable because this is not a hosting service. However the deployment process for AT&T Intrusion Detection/Prevention service is Step 1 – Data Collection Step 2 – Milestone Notification Step 3 – Preparing Your Environment Step 4 – Equipment Installation Step 5 - Test and Turn-up Step 6 – Transition Service(s) into Maintenance Step 7 – Service Completion Notice
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

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).

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	Storage is only applicable for recording of calls via Webex. Storage can be purchased on a per gig basis as part of the service.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Some of this will not apply with Blue Jeans because we are 100% cloud based and will never deploy new servers on the customer premise. Furthermore we do offer Command Center Pro as our industry leading VaaS monitoring tool.
AT&T Cloud Web Security Service	IaaS	N/A	AT&T Cloud Web Security Service is provided as a SaaS on a per seat/user basis inclusive of all cloud servers, images, storage, and tools to monitor and report on customer's environment. AT&T Cloud Web Security Service provides network-based (cloud) web filtering, malware and content scanning of Customer-designated network users or devices, including roaming (not connected to Customer VPN) and mobile user support. AT&T is acting in its capacity as a data processor and will process the Traffic Data of Customer only on behalf of and under the direction of Customer (and its designees).
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Service is provided as a SaaS on a per seat/user basis inclusive of all cloud servers, images, storage, and tools to monitor and report on customer's environment. AT&T provides network-based (cloud) web filtering, malware and content scanning of Customer-designated network users or devices, including roaming (not connected to Customer VPN) and mobile user support. AT&T is acting in its capacity as a data processor and will process the Traffic Data of Customer only on behalf of and under the direction of Customer (and its designs).

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Hosted Contact Center Service	SaaS	Yes	inContact is constantly evaluating the status of our network and how "saturated" it is. Because of this we are constantly adding additional capacity as needed, to support our customers. In addition, inContact routinely includes a capacity notification alert when setting up a customer. For example, when 80% or 85% utilization occurs the system will contact a designated distribution list with a warning that capacity is running out and where to reach out for assistance. In addition, inContact can rapidly add additional capacity as needed with a simple phone request to either a designated Service Delivery Manager or our 24x7 Tech Support line. System Utilization is monitored around the clock: SolarWinds, IPMonitor watching network, drive space and Trunking capacities are monitored continually, SSMon and Equinox - We have a dedicated resource at inContact who studies capacity. We also have capacity thresholds and alerting mechanisms, which trigger capacity growth when we hit those triggers – for example 50% capacity on media servers will trigger the creation of additional media servers. We have a 7 x 24 NOC with eyes on these alerts. The Utilization study is done real time and is automated with capacity metric triggers. System Utilization is continual and automated with predefined threshold triggers. Item #4 is Not Applicable for our "True" multi-tenant cloud solution
AT&T Premises-Based Firewall Service	IaaS	No	Not applicable to a managed firewall service because servers and other computing resources are not being delivered.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	No	Not applicable to a managed IDS/IPS service because servers and other computing resources are not being delivered.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	ACDN does not host origin content. All content is placed by the consumer of cloud services on what itself feels is cacheable in storage. As such, ACDN does not rely on origin infrastructure. In fact many clients switching from one cloud hosting provider to another place ACDN out in front for a 100% availability of cached content even if the origin server suffered an

AT&T Product	Category	Comply (yes/no)	AT&T Response
			outage. The customer may purge all content guaranteed within five minutes CONUS and 95% OCONUS on its platform. Customer maintains who holds access via the LUNA portal to add, modify or change content and determines the Time to Life (TTL) of every element of their properties on ACDN They also can maintain their own selections for Firewall rule sets and multiple modes (Deny, Alert or Allow) via clicks in the portal. ACDN gives control to the end user from more than just the data center front door inward. ACDN gives control to the end point where the user touches the Internet.

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

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T can provide 15 day or 60 day trial for our Webex and AT&T Conferencing offer.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	During the Blue Jeans 14 day trial period we can offer a Proof of Concept to test various connectivity options such as Room Systems, Lync/Skype for Business, PSTN, Jabber, WebRTC, Browser, Desktop Application, iOS and Android. Furthermore, once a Blue Jeans customer depending on the deal, we can offer a dedicated Customer Success Manager to assist in implementation, roll out, and training.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T offers at no charge the Trial Service Components for 30 users for a 30 day period as part of our standard contract on an opted out basis.
AT&T Distributed	IaaS	See	AT&T DDoS service does not offer a testing/training

AT&T Product	Category	Comply (yes/no)	AT&T Response
Denial of Service (DDoS) Defense Service		Comment	period.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T can provide a trial for Unified Communications Services for 30-60 days based on client requirements.
AT&T Hosted Contact Center Service	SaaS	Yes	Towards development completion, our development team will install software in a test environment and encourage joint client testing. Typically the testing process occurs during the final weeks of development. Upon completion of Testing, we will walk purchasing entity through the complete installation and setup of their application. Once installed on the production servers, comprehensive training may be extended to the client's IT/ MIS personnel; not only to administer and maintain it, but also to understand the underlying technology and development tools. After successful implementation, we will stay on the project during Beta rollout, monitoring the application, reviewing failed call transactions, tuning the grammars, making necessary application changes and ensuring that the system achieves the desired quality and results. **Rollout** Once the IVR is performing to inContact and purchasing entity 's satisfaction, we will remain vigilant during the commercial rollout and continue to monitor for at least two weeks to iron out any remaining issues that may surface. Standard support and maintenance will follow. **Training**: inContact provides our customers with a training plan flexible enough to meet the needs of each organization. End-users and staff will have access to our inContact University that provides users with self-paced learning modules that can be accessed through the web from anywhere at any time. inContact also offers a train-the-trainer program during our Enterprise implementation that is delivered via live instructor virtually or it can be substituted for a class-room based session. Our implementation training is designed to help ensure success and prepare our clients for launch. The live instructor-led courseware consists of several module options:

AT&T Product	Category	Comply (yes/no)	AT&T Response
			• Agent Module • Management and Administration • Reporting • Introduction to development
AT&T Premises-Based Firewall Service	IaaS	See Comment	Based on the MSS Service that you have selected, the SIM or Managed Security Operations Center (MSOC) will review the firewall and/or IDPS policy with you prior to turn-up completion and acceptance into maintenance. At this stage, your circuit, firewall and/or IDPS are considered successfully installed. An email and phone call from your SIM confirms your site is in maintenance and includes information for contacting the MSOC. You will also receive a welcome letter from the MSOC with additional details on support of your AT&T Managed Security Service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Based on the MSS Service that you have selected, the SIM or Managed Security Operations Center (MSOC) will review the firewall and/or IDPS policy with you prior to turn-up completion and acceptance into maintenance. At this stage, your circuit, firewall and/or IDPS are considered successfully installed. An email and phone call from your SIM confirms your site is in maintenance and includes information for contacting the MSOC. You will also receive a welcome letter from the MSOC with additional details on support of your AT&T Managed Security Service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Training options include regional classroom training, on-line training, and custom on-site training. Testing specific to a customer implementation is provided as a standard part of the available installation/integration services detailed on question 84. The integration and on-boarding is a fully managed project including testing periods (i.e. alert mode vs deny mode for attack mitigation) and tuning prior to production to help ensure the service is fully operational.

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.

AT&T Response:

AT&T Conferencing with Cisco WebEx and the AT&T Video Meetings with Blue Jeans offers a two-week trial period. The trial environment for AT&T Unified Communications as a Service is 30 -45 days.

AT&T will work with the Participating Entity to determine availability of any additional test and/or proof of concept environments for the additional products proposed in our response.

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

AT&T Response:

AT&T shall provide access to technical documentation as it relates to the system features and services, system administration and training documentation at no cost. This documentation can be in the form of webinars with links to technical and system administration documentation.

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.

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	WebEx® is software as a service (SaaS) that we deliver via a highly secure and reliable enterprise network. We can deploy it quickly, in a matter of weeks instead

AT&T Product	Category	Comply (yes/no)	AT&T Response
			of months, so you can easily scale the service to meet your changing needs. And, the cloud-based service connects you instantly to the nearest data center. If a data center experiences network congestion or interruption, the service reroutes your connection smoothly to the next nearest data center. Because it's compatible with a variety of equipment, WebEx® gives you many endpoint options. You can use desktop or laptop computers or supported mobile devices such as many versions of iPhone®, iPad®, Android™, and BlackBerry®.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans offers a full suite of APIs to build integrations as needed. Furthermore, we do have prebuild integrations with certain Learning Management Services as well as UC Chat clients. We also offer the ability to embed video directly into a custom web portal for further integrations.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security can integrate with a log management system through standard-based interfaces.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	Integration can mean different things to different people. In some cases, integration means to embed a piece of an application within another application. In other cases, integration may simply mean a method of communication between the two platforms. AT&T UC would require an integration meeting to discuss the requirements and abilities to integrate with other multi-portal devices. AT&T UC offers various methods for integrating with third-party software, such as Salesforce.com, Microsoft, Google etc. allowing seamless transport of data between platforms.
AT&T Hosted Contact Center Service	SaaS	Yes	Integration can mean different things to different people. In some cases, integration means to embed a piece of an application within another application. In other cases, integration may simply mean a method of communication between the two platforms. With this in mind, inContact would require an integration meeting to discuss the requirements and abilities to integrate with other multi-portal devices. inContact offers various methods for integrating with

AT&T Product	Category	Comply (yes/no)	AT&T Response
			third-party software, allowing seamless transport of data between platforms within your contact center, and increased agent productivity. inContact provides CTI capabilities through inContact Studio, our drag and drop programming tool. inContact Studio is an application that was built in such a way to make it easy for both the programmer and the non-programmer to be able to interact with the system. inContact Studio is also capable of passing information via customizable URL screen pops or a customizable command line screen pop, from the inContact suite to the agents desktop.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	The ACDN service perfectly integrates with any standard SIEM for logging. Also, API's/interfaces are provided for handling cache purges, DNS zone transfers etc.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	The AT&T Conferencing with Cisco WebEx solution is specifically built in a custom manner to meet the requirements or our customers. Individual customers have specific locations with user requirements that are reviewed at the beginning of any planning or

AT&T Product	Category	Comply (yes/no)	AT&T Response
			implementation effort, and those requirements are built into the overall solution.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Enterprise Groups have the option to customize their Blue Jeans experience, with features such as customizing the dial-in phone numbers that appear in email invitations and meeting web app. This can be done at the Enterprise Group level (by the Admin) or at the Account level (by the account user). Two other customizations, that can be done at the back-end by Blue Jeans support, are: • Replacing the Blue Jeans logo with your own brand. Your custom logo will appear in: - Your Blue Jeans account web pages, - Email invitations (created from the BJN web page. Outlook invites will not show logo). - Inside your meeting when joining from the Browser Plugin, WebRTC, and the Blue Jeans App. Logo will also appear in your custom landing page (CLP), if you have one. • Adding customized text to your meeting invitation emails. Blue Jeans is open to discuss any other customization needs.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security allows each participating entity to customize and personalize the blocked website warning page with local information and purchasing entity logo.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	There is an element of customization with DDoS Service in that the DDoS Threat Team customizes the configuration to meet the customer's DDoS requirements.
AT&T Unified Communications as a Service	SaaS	Yes	The UC solution is specifically built in a custom manner to meet the requirements or our customers. Individual customers have specific locations with user requirements that are reviewed at the beginning of any planning or implementation effort, and those requirements are built into the overall solution.
AT&T Hosted Contact Center Service	SaaS	Yes	There are numerous customization options which can be made with inContact's software solutions. Accessibility to customization may be granted or denied, per a user's designated Security Profile. The inContact platform provides users with the flexibility to customize their contact center to meet any requirement they have. Individual skills can be

AT&T Product	Category	Comply (yes/no)	AT&T Response
			configured to provide unique call flow experiences including customized integrations for distinct business groups. At the core of inContact is the inContact Studio application designer, also known as the Script Editor. This program is a tool to design simple or complex applications for voice, email, chat, fax, or a combination of all. Nearly every inContact Studio feature can be implemented from within a custom application. This includes automated call distribution (ACD), interactive voice response (IVR), call-back, voice mail, text-to-speech, email notification, and many others. inContact Studio is tailored to meet the needs of experienced software engineers as well as give the novice developer the ability to create a simple call flow through an intuitive, easy to understand interface. inContact's Developer Portal and Developer's Community provides the next level of customization and integration for our platform. Access will be provided to our easy to understand APIs using our Developer Portal, a resource that helps your developers keep up to date on how the APIs work and how they can speed up their integration and development projects. The Developer Portal allows programmers to exercise each of our more than 120 published APIs. They get access to complete documentation on the APIs including reference guides, SDK tutorials with sample application code and interactive, online documentation for every RESTful API in the inContact platform. We also provide FAQs and tutorials on best practices for developing REST-based applications and SDK solutions. The inContact API Framework is a collection of RESTful APIs that provide access to inContact data and services. The RESTful API requests are all made over HTTPS. The Agent SDK shows how to use the Agent API to create fully-functional agent applications. A guide is provided that describes important concepts on the inContact platform. A sample HTML application is also provided that shows how to use the Agent API from JavaScript. The Agent API can be used to create stand-alone agent applications, or to embed agent functionality in other applications (like CRMs). For

AT&T Product	Category	Comply (yes/no)	AT&T Response
			example, the inContact Agent Console for Salesforce.com was developed using the Agent API.
AT&T Premises-Based Firewall Service	IaaS	Yes	Each client will receive pre-sales technical support for proper sizing and selection of the required components to deliver the proper service. Manufacturer preferences can be exercised as well as a number of options to address specific client requirements.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Each client will receive pre-sales technical support for proper sizing and selection of the required components to deliver the proper service. Manufacturer preferences can be exercised as well as a number of options to address specific client requirements.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	Based on the specific requirements, AT&T Professional Services can design and develop solutions that can be deployed at the ACDN edge – making the development cycle faster and cost effective. Our experts use proven methodologies to help move faster, unleashing the power of the ACDN Platform for your business. ACDN experts have helped some of the most dynamic, interactive and engaging Web properties on the Internet keep up with the changing online environment, and stay lightning fast at the same time. Some of the capabilities include: performance testing and tuning, automate workflow, online event management, project management, third party load testing, end user validation failover solutions, custom reporting and analytics, geo-targeting, mobile device identification, A/B testing, user prioritized access, private content delivery networks. Security capabilities: traffic filtering, configuration assistance, end user validation, geo targeting, proactive security event monitoring, security event after action reporting, security incident management, threat update reviews, table top attack drills and customized vulnerability scanning and analysis

8.20 (E) MARKETING PLAN

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

AT&T Response:

AT&T has a dedicated team of marketing professionals specifically aligned to service the government vertical. These individuals develop content around the wide variety of AT&T cloud based solutions and craft the messaging to meet the business needs of the participating entities. Utilizing the power of the AT&T brand, we bring to market messaging via print, electronic and social media outlets to tell the AT&T cloud based solutions story and articulate the value of AT&T as an integrated solutions provider.

AT&T will work with closely with NASPO ValuePoint to develop a cohesive marketing strategy for the participating members to maximize the benefit of the cloud based solutions portfolio.

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.

AT&T Response:

AT&T is constantly refining its product mix and anticipates being able to deliver enhanced services over time. Additionally, AT&T Consulting can advise Purchasing Organizations on how best to leverage services and optimize the synergy between them.

Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Cisco WEbex integrates directly with AT&T Cisco UC Voice telephony in the cloud offer. Cisco Jabber and one touch conferencing is available as a combined service

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans and AT&T has the ability to diagnose network issues and help identify network challenges. Blue Jeans also assigns a customer success manager for support on deployment, training and troubleshooting. This greatly help with customer success and satisfaction.
AT&T Cloud Web Security Service	IaaS	Yes	In addition to the services that are provided during implementation and ongoing support of the service the following professional security services are available: • Security Strategy and Roadmap • Governance, Risk and Compliance • Payment Card Industry Solutions • Secure Infrastructure Services • Vulnerability and Threat Management Application Security Services
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	Yes	In addition to the services that are provided during implementation and ongoing support of the service the following professional security services are available: • Security Strategy and Roadmap • Governance, Risk and Compliance • Payment Card Industry Solutions • Secure Infrastructure Services • Vulnerability and Threat Management Application Security Services
AT&T Unified Communications as a Service	SaaS	Yes	**UC and Telephony Together in the Cloud** AT&T UC Services provides users with one place to go for enhanced visibility and control over a range of UC applications and telephone features. Two tightly integrated components comprise this offering, including AT&T Unified Communications Voice (AT&T UC Voice) and Cisco Jabber®. AT&T UC Voice is a feature-rich, cloud-based IP telephony solution that provides easy-to-use, high-quality voice and UC features as-a-service. It employs the Cisco Hosted Collaboration Solution (HCS) platform as the core of this service. Cisco Jabber® is a UC client application for a selection of mobile devices, smart devices and PCs. It provides an easy-to-use dashboard for a consolidated view into multiple UC and IP Telephone tools. These services are offered in a number of packages,

AT&T Product	Category	Comply (yes/no)	AT&T Response
			providing you with the flexibility to mix and match and select those that best meet your needs. Current packages include: • **Essential** Includes voice and basic call processing. Generally used for common areas such as conference rooms and lobby areas, as well as support for • traditional analog phones. Voicemail is not available with this package. • **Fundamental** Includes voice and basic call processing and Single Number Reach (SNR). Voicemail can be added as an optional feature. • **Fundamental with Cisco Jabber ®** Includes voice and basic call processing for a single Cisco Jabber® mobile or desktop client, SNR, and voicemail. Jabber® client can be installed on up to 10 devices. • **Basic** Includes voice and basic call processing and SNR for a single IP hard phone. Voicemail can be added as an optional feature. • **Standard with Cisco Jabber®** Includes voice and basic call processing, SNR and a single Cisco Jabber® softphone client (desktop or mobile). Voicemail can be added as an optional feature. • **Enhanced with Cisco Jabber®** Includes voice and basic call processing, SNR, Cisco Jabber® client for up to 10 devices (softphones and hard phones each count as one device), and unified messaging (includes voicemail). • **Enhanced with Cisco UC Integration for Microsoft® Lync®** Includes voice and basic call processing, SNR, and Cisco UC Integration for Microsoft® Lync® (CUCILync) for integration to Microsoft® Lync® UC client*, and unified messaging (includes voicemail). **Microsoft® Lync® UC client not provided as part of the package.* A device can consist of an Internet Protocol (IP) phone, desktop client, mobile client, or analog device. No devices are included in the bundles.
AT&T Hosted Contact Center Service	SaaS	Yes	inContact provides a variety of services both pre and post install. Pre engagement services include "business consulting", where our BCO organization will study work and call flow of an agency/entity along with desired business outcomes/success metrics, and provide a detailed plan and report as to how the

AT&T Product	Category	Comply (yes/no)	AT&T Response
			inContact solution should be configured to achieve the desired results. Post installation, inContact provides several ongoing training programs, both web based (on demand), webinar based, and instructor led either onsite at customer site, or in our Salt Lake City UT training facility. Also, inContact provides many customer events during the year, such as the annual ICUC inContact Users Conference, held in the fall each year.
AT&T Premises-Based Firewall Service	IaaS	Yes	In addition to the services that are provided during implementation and ongoing support of the service the following professional security services are available: • Security Strategy and Roadmap • Governance, Risk and Compliance • Payment Card Industry Solutions • Secure Infrastructure Services • Vulnerability and Threat Management • Application Security Services
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	In addition to the services that are provided during implementation and ongoing support of the service the following professional security services are available: • Security Strategy and Roadmap • Governance, Risk and Compliance • Payment Card Industry Solutions • Secure Infrastructure Services • Vulnerability and Threat Management • Application Security Services
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN provides anywhere from a fully self-serviceable interface to a complete turnkey service to our customers. From a security perspective, customers have the ability to handle all security events themselves or have AT&T provide a managed security service to them. AT&T also offers services like threat advisory, consulting, training etc. to our customers.

8.22 (E) SUPPORTING INFRASTRUCTURE

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

AT&T Response:

The AT&T cloud based services offering is truly scalable based on the needs of the Purchasing Entity and contains a variety of products and services to choose from to meet those needs. Each of the products and services submitted under this solicitation has different infrastructure and systemic requirements based on implementation of the solution.

AT&T works closely with the participating entity to determine existing entity infrastructure meets the needs of the cloud based solution being procured.

Due to the individual variances for each Purchasing Entity, each Purchasing Entity's requirements will need to be assessed at the time of service ordering. As a general guideline, we include the following guidance for the products we propose.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T Webex Solution is hosted in Tier 3 or Tier 4 data center facilities. AT&T provides our Webex Services in a hosted multi-tenant environment that manages multiple customers from a single management space. Infrastructure controls are specifically designed to compartmentalize customer data. Access from one customer environment to another is not permitted.
AT&T Video Meetings with Blue Jeans	SaaS		As a cloud-based service, infrastructure is not required by the Purchasing Entity; however, network connectivity is required.
AT&T Cloud Web Security Service	IaaS	Yes	Customer may choose from numerous connections methods which include Explicit Proxy, Firewall VPN (IPSec), Mobile Client Connector, Apple Mobile Device, and Proxy Forwarding. Each connection method may require additional customer equipment or configuration of customer equipment which will be determined at time of installation. Customer can also choose to integrate with Active Directory and which requires a member servers of the domain to host the connector software. Customer must provide their own internet access.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	The Customer needs at least one (1) ISP and IP address. They need to ability to support BGP and at least one (1) VPN.
AT&T Unified Communications as a Service	SaaS	Yes	AT&T UC Voice is hosted in our Watertown, MA and Allen, TX Internet Data Centers. These facilities meet the Tier 3 or Tier 4 data center facilities AT&T provides our UC Services in a hosted multi-tenant environment that manages multiple customers from a single management space. Infrastructure controls are specifically designed to compartmentalize customer data. Access from one customer environment to another is not permitted other than through traditional PSTN connections
AT&T Hosted Contact Center Service	SaaS	Yes	As a cloud-based service, infrastructure is not required by the Purchasing Entity; however, network connectivity is required.
AT&T Premises-Based Firewall Service	IaaS	Yes	Customer needs to allocate data center floor space and provide network connectivity along with a POTS line for out-of-band management.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	Yes	Customer needs to allocate data center floor space and provide network connectivity along with a POTS line for out-of-band management.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	As a cloud-based service, infrastructure is not required by the Purchasing Entity; however, network connectivity is required.

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

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing	SaaS	Yes	All costs will be identified on pricing lists, and/or

AT&T Product	Category	Comply (yes/no)	AT&T Response
with Cisco WebEx			resulting detailed quote/contract. Responsibilities will be clearly outlined and identified during the SOW process, prior to work commencement.
AT&T Video Meetings with Blue Jeans	SaaS	Yes	Blue Jeans is a cloud-based only infrastructure which acts as the service to provide video conferencing. If Blue Jeans Relay is deployed, we offer free software to be installed locally to manage the room systems.
AT&T Cloud Web Security Service	IaaS	N/A	All costs will be identified on pricing lists, and/or resulting detailed quote/contract. Responsibilities will be clearly outlined and identified during the SOW process, prior to work commencement.
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	N/A	Not applicable to DDoS service.
AT&T Unified Communications as a Service	SaaS	Yes	All costs will be identified on pricing lists, and/or resulting detailed quote/contract. Responsibilities will be clearly outlined and identified during the SOW process, prior to work commencement.
AT&T Hosted Contact Center Service	SaaS	Yes	All costs will be identified on pricing lists, and/or resulting detailed quote/contract. Responsibilities will be clearly outlined and identified during the SOW process, prior to work commencement.
AT&T Premises-Based Firewall Service	IaaS	See Comment	Not applicable to a managed firewall service because no on demand services that might require expansion are being offered.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	Not applicable to a managed IDS/IPS service because no on-demand services that might require expansion are being offered.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	N/A	

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).

AT&T Response:

AT&T has read and understands. Please refer to the table below for our product-specific responses to this requirement.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Conferencing with Cisco WebEx	SaaS	Yes	AT&T's solution is implemented and operated in accordance with the security controls, guidelines, and standards, to the extent applicable, listed in the sections of Security Requirements and Information Use and Disclosure- Standards. AT&T has a significant amount of demonstrated expertise and experience in the delivery of systems that are implemented and operated in accordance with FISMA, NIST SP 800- 53, CJIS and IRS 1075 security controls. http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx.
AT&T Video Meetings with Blue Jeans	SaaS	See Comment	In referencing http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 the Blue Jeans cloud would be designed in a similar manner. Our cloud is also comprised of separate layers (or actors) for certain functionality. These layers include the client facing proxy later which allows/disallows connections to the BJN Cloud. Secondly, there is another protected layer for media and web traffic. Finally, there is a third protected layer which supports application and database servers.
AT&T Cloud Web Security Service	IaaS	Yes	AT&T Cloud Web Security Service aligns with Software as a Service (SaaS).
AT&T Distributed Denial of Service (DDoS) Defense Service	IaaS	See Comment	DDoS service generally complies with the NIST 800-145 definition of PaaS.

AT&T Product	Category	Comply (yes/no)	AT&T Response
AT&T Unified Communications as a Service	SaaS	Yes	AT&T's solution is implemented and operated in accordance with the security controls, guidelines, and standards, to the extent applicable, listed in the sections of Security Requirements and Information Use and Disclosure- Standards. AT&T has a significant amount of demonstrated expertise and experience in the delivery of systems that are implemented and operated in accordance with FISMA, NIST SP 800-53, CJIS and IRS 1075 security controls. http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx
AT&T Hosted Contact Center Service	SaaS	See Comment	inContact is representative as Software as a Service, and more aligns with Platform as a Service (SaaS), but not in every respect, being SaaS
AT&T Premises-Based Firewall Service	IaaS	See Comment	The closest alignment is IaaS but as a managed service the self-provisioning, self-management and on-demand nature is not applicable.
AT&T Managed Intrusion Detection/Intrusion Prevention Service	IaaS	See Comment	The closest alignment is IaaS but as a managed service the self-provisioning, self-management and on-demand nature is not applicable.
AT&T Professional Services	IaaS	N/A	
AT&T Content Delivery Network Service	IaaS	Yes	ACDN adheres to the FedRAMP Moderate Level II JAB P-ATO standards of cloud computing, which incorporates the NIST series mentioned here. It additionally brings 256 additional controls and a requirement for continuous monitoring, not just an annual audit.

7. Confidential, Protected or Proprietary Information

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write “None” in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

3.13 CONFIDENTIAL OR PROPRIETARY INFORMATION

The Government Records Access and Management Act (GRAMA), UCA § 63G-2-305, provides in part that:

the following records are protected if properly classified by a government entity:

(1) *trade secrets as defined in Section 13-24-2, the Utah Uniform Trade Secrets Act, if the person submitting the trade secret has provided the governmental entity with the information specified in UCA § 63G-2-309 (Business Confidentiality Claims);*

(2) commercial information or non-individual financial information obtained from a person if:

(a) *disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future;*

(b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access; and

(c) the person submitting the information has provided the governmental entity with the information specified in UCA § 63G-2-309;

** * * * **

(6) records, the disclosure of which would impair governmental procurement proceedings or give an unfair advantage to any person proposing to enter into a contract or agreement with a governmental entity, except, subject to Subsections (1) and (2), that this Subsection (6) does not restrict the right of a person to have access to, after the contract or grant has been awarded and signed by all parties, ...

Pricing may not be classified as confidential or protected and will be considered public information after award of the contract.

Process for Requesting Non-Disclosure: Any Offeror requesting that a record be protected shall include with the proposal a Claim of Business Confidentiality. To protect information under a Claim of Business Confidentiality, the Offeror must complete the Claim of Business Confidentiality form with the following information:

1. Provide a written Claim of Business Confidentiality at the time the information (proposal) is provided to the state, and
2. Include a concise statement of reasons supporting the claim of business confidentiality (UCA § 63G-2-309(1)).
3. Submit an electronic "redacted" (excluding protected information) copy of the record. The redacted copy must clearly be marked "Redacted Version."

The Claim of Business Confidentiality Form may be accessed at:
http://www.purchasing.utah.gov/contract/documents/confidentialityclaimform.doc

An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY", and if so identified, shall be considered non-responsive unless the Offeror removes the designation.

Redacted Copy: If an Offeror submits a proposal that contains information claimed to be business confidential or protected information, the Offeror must submit two separate proposals: one redacted version for public release, with all protected business confidential information either blacked-out or removed, clearly marked as "Redacted Version"; and one non- redacted version for evaluation purposes, clearly marked as "Protected Business Confidential."

The Lead State and NASPO ValuePoint are not liable or responsible for the disclosure of any confidential or proprietary information if the Offeror fails to follow the instructions of this section.

AT&T Response:

None.

8. Exceptions and/or Additions to the Standard Terms and Conditions.

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

AT&T Response:

AT&T outlines the contact information for the person(s) that will be directly involved in terms and conditions negotiations in the table that follows.

Name	Title	Phone Number	Email
Rick Frankhuizen	Senior Customer Contract Manager	661-263-9835	wf2146@att.com
Ron Montague	Senior Customer Contract Manager	425-749-2455	rx7908@att.com
Susan Lord	Executive Director, Senior Legal Counsel	214-757-7587	sl2192@att.com

We provide any exceptions and/or additions to the Main RFP document in the table below. We include the Section reference and our explanation.

Section	Explanation
5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.	The undersigned's is unaware of a disqualification or debarment that would negatively affect our ability to provide the products and services. At AT&T, we commit to fully complying with state and Federal regulations.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.

Section	Explanation
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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).	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
8.6.7 Offeror must describe whether it can	Please refer to Attachment E, AT&T Information &

Section	Explanation
restrict visibility of cloud hosted data and documents to specific users or groups.	Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide. AT&T does not disclose the specific encryption technologies that it deploys. AT&T does make use of industry standard and accepted encryption technologies in the deployment of its services
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.	AT&T understands the requirements to fully protect the privacy of patient medical data and will take reasonable steps to assist NASPO in maintaining compliance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) regulations. In its role of telecommunications provider, however, AT&T by definition is not, nor could it be considered, a “Business Associate” of a “Covered Entity” under HIPAA regulations and, therefore, may only agree to assist MPIPHP in any reasonable manner in its compliance efforts. A Business Associate agreement is not appropriate for this project. To the extent AT&T has access to “individually identifiable” patient health information, AT&T agrees that such information shall be treated as confidential and shall not be disclosed to anyone who does not need that information to perform

Section	Explanation
	his/her professional duties.
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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide. AT&T makes use of the traffic flowing across its network for capacity planning and traffic management.
8.11 (E) DATA DISPOSAL Specify your data disposal procedures and policies and destruction confirmation process.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.
8.13 (E) CLOUD SECURITY ALLIANCE Describe your level of disclosure with CSA Star Registry for each Solution offered. a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.53 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.	Please refer to Attachment E, AT&T Information & Network Security Customer Reference Guide.

Additionally, AT&T notes any exceptions and/or additions to the RFP Attachment A and Exhibits 1, 2, and 3, directly in the attachments and embed the files below for easy reference.

1-ATT Exceptions-Addition

2-ATT Exceptions-Addition

3-ATT Exceptions-Addition

4-ATT Exceptions-Addition

9. Cost Proposal

Cost will be evaluated independently from the technical proposal. Offeror's cost proposal must include the items discussed in Section 9 of the RFP.

Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5).

All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.

AT&T Response:

AT&T understands.

9 COST PROPOSAL

9.1 (M) COST PROPOSAL

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's' commercially published pricelists versus fixed pricing. In addition, Offerors must have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

Offeror must identify its cost proposal, Attachment G, as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement, as allowed by the Lead State.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent to of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, overhead, and any other costs related to the service. The specific rate (within a range) charged for each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

AT&T Response:

AT&T understands. Please refer to our separate pricing file titled *ATT_Cost Proposal–CH16012 Cloud Solutions.xlsx*.