Contract #: AR3113

STATE OF UTAH COOPERATIVE CONTRACT

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

Presidio Networked Solutions LLC.
Name

8161 Maple Lawn Boulevard, Suite 150
Street Address

Fulton	MD	20759
City	*State*	*Zip*

Vendor # VC226563 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* Trina Dennis-Carlson *Phone Number:* 301-623-1872 *Email:* tdennis-carlson@presidio.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Thursday, August 01, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

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

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLA

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

9. 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 Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. 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. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Trina Dennis-Carlson 8/9/19
Contractor's signature Date

Trina Dennis-Carlson, Director Contracts
Type or Print Name and Title

DIVISION OF PURCHASING

Aug 9, 2019
Director, Division of Purchasing Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

Data means all information, whether in oral or written (including electronic) form,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

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

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

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

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

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

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

Security Incident means the possible or actual unauthorized access to a Purchasing

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

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

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

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

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

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

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/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision 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 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.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

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

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

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

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and 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 Purchasing Entity under the applicable commercial code.

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

12. Force Majeure: Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification and Limitation of Liability

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

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against third party claims, damages or causes of action including reasonable attorneys' fees and related costs to the extent directly resulting from a claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from; (a)the combination of the Product with any other product, system or method, (b) the alteration or modification of the Product, or (c) any use of the Product not conforming to the Product specifications for use unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending

the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

(3) Should any third-party provided Product become (or in Contractor's or such third party's opinion be likely to become) the subject of an Intellectual Property Claim, the Contractor shall pass-through the applicable third-remedy for such Intellectual Property Claim. Should any Contractor Product become (or in Contractor's opinion be likely to become) the subject of an Intellectual Property Claim, Contractor shall at its sole option and expense: (i) procure for Company the right to continue using the relevant Product; (ii) replace or modify the Product so that it becomes non-infringing provided that any replacement of modified Product meets substantially the same specifications as the originally provided Product; or (iii) if neither of the foregoing alternatives is reasonably available provide a credit to applicable Indemnified Party the price paid to Contractor for such Product as depreciated or amortized by an equal amount over the lifetime of the Product as established by Contractor.

This Section states Contractor's entire liability, and Indemnified Party's sole and exclusive remedy, with respect to infringement of Intellectual Property Rights claims. The foregoing is given to the Indemnified Party in lieu of all warranties of non-infringement with respect to the Products.

(c) LIMITATION OF LIABILITY.
i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five million dollars ($5,000,000), whichever is greater.

ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall

demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in this section will not apply to claims for bodily injury or death as set forth in Section 13, and Section 31 – Data Privacy when made applicable under a specific purchase order.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

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 the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

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

b. Coverage shall be written on a claims-made basis. The minimum acceptable limits shall be as indicated below, any deductible paid by Contractor for each of the following categories:

(1) Commercial General Liability covering premises operations, independent

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

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

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

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

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

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing

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

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

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

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

b. 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. 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. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

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

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

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

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration 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.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any

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

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

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

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

---

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

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

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

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

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

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

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

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to

or more stringent than those specified in the Solicitation.

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

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

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

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

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

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

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

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

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

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

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

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

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

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

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

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 JAGGAER, formerly SciQuest, whereby JAGGAER 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://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

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

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

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

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

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

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or

whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

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

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X	X	X	All

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: Presidio Networked Solutions, LLC

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. 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.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
AWS	1.15%
Azure	1.00%
Average SaaS OEM Discount Off	**1.08%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		$100-$250	$120-$300	$100-$250	$120-$300
Professional Services					
	Deployment Services	$100-$250	$120-$300	$100-$250	$120-$300
	Integration Services)	$100-$250	$120-$300	$100-$250	$120-$300
	Consulting/Advisory Services	$100-$250	$120-$300	$100-$250	$120-$300
	Architectural Design Services	$100-$250	$120-$300	$100-$250	$120-$300
	Statement of Work Services	$100-$250	$120-$300	$100-$250	$120-$300
Partner Services		$100-$250	$120-$300	$100-$250	$120-$300
Training Deployment Services		$100-$250	$120-$300	$100-$250	$120-$300
Professional Consultant Rates (Hourly)					
	Associate Engineer (Tier 1)	$ 100.00	$ 120.00	$ 100.00	$ 120.00
	Staff Engineer (Tier 2)	$ 130.00	$ 156.00	$ 130.00	$ 156.00
	Sr. Engineer (Tier 3)	$ 175.00	$ 210.00	$ 175.00	$ 210.00
	Principal Engineer (Tier 4)	$ 200.00	$ 240.00	$ 200.00	$ 240.00
	Architect (Tier 5)	$ 225.00	$ 270.00	$ 225.00	$ 270.00
	Principal Consultant (Tier 6)	$ 250.00	$ 300.00	$ 250.00	$ 300.00
	Project Manager	$ 175.00	$ 210.00	$ 175.00	$ 210.00

6. Technical Response

A. Proposed Cloud Solutions

The AWS and Azure platforms, and their services and micro services, offer cloud solutions featuring a combination of manual and automated controls. Both cloud platforms are well suited for maintaining and automating several processes in the cloud pillars of Networking, Storage, Compute, Security, and DevOps. This combination of monitoring and Identity Access Management policies will be used to provide role-based client controls.

Additionally, containers on the public cloud provide flexibility for running both existing and cloud-native applications on physical and virtual infrastructure. Containers package up the services comprising an application and make them portable across different compute environments, for both dev/test and production use. With containers, clients can quickly ramp application instances to match spikes in demand. In addition, because containers draw on resources of the host Operating System (OS), they are much lighter weight than virtual machines. This means containers make highly efficient use of the underlying server infrastructure.

Presidio takes an "automation first" approach to all of our implementations. This means we will use tools and capabilities such as configuration management, continuous integration/continuous delivery (CI/CD), and automated testing to enable rapid release of capability to our customers. This enables us to meet our customers' evolving needs while lowering the cost/operational overhead associated with change. Additionally, our automation solutions allow us to scale from an initially "small" footprint for development/test environments all the way up to elastic production workloads with full HA/DR. Our automation first approach ensures security concerns are addressed. Minimizing access between core components and services, while incorporating tight access control and end-to-end encryption to protect sensitive infrastructure data, is tightly integrated into the DNA of our automated pipelines.

We begin with an analysis of the desired workloads, expected production volume, and existing tools. Based on this analysis, we create a plan that identifies the need for any new tools and capabilities, in addition to implementing, integrating, securing, and deploying missing capabilities. This may include simple projects, such as implementing a solution to secure keys, to more complex projects that encompass deploying a full-scale cloud native platform. We then incrementally build and deploy integrated capabilities to enable downstream work to proceed (application development) while the platform is enhanced and scaled. Finally, our automation first approach means all work is codified, version controlled, and tested prior to implementation without human intervention. This transparency enables application development teams to utilize production-like environments and tools for development, and accelerate their development lifecycle.

Presidio has a deep, mobile skillset in its Consulting, Cloud Integration, and Software Development groups (Exhibit 6-1) and offers a combination of solutions from hybrid cloud design to security and cloud migration services. We help enable our clients to embrace a DevOps and Agile methodology for deployment of customer environments, internal systems, non-production systems, and to ensure continuation post-migration. We will also work to ensure

standardization across all environments as it relates to best practices, configuration management, and deployment strategies. Our vision is a holistic approach to business, technology, and people/processes.

Exhibit 6-1. Presidio's Comprehensive Portfolio of Cloud Consulting, Integration, and Software Development Service Capabilities

B. Responses to RFP Section 8 Technical Requirements

8 TECHNICAL REQUIREMENTS

If applicable to an Offeror's Solution, an Offeror must provide a point by point response 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.

Response:

Presidio complies. Our point-by-point responses to the RFP Section 8 Technical Requirements follow.

8.1 (M)(E) TECHNICAL REQUIREMENTS

8.1.1 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 characteristics defined in NIST Special Publication 800-145.

Response:

For a detailed information concerning the proposed AWS and Azure cloud solutions' compliance with the characteristics defined in NIST Special Publication 800-145, please refer to our previous response to RFP section 6.5.3 in the document entitled, "Presidio Business Information.pdf" uploaded in response to #2.1.5 in the SciQuest portal.

A brief summary for each service delivery model follows:

- **SaaS:** Sourced via the AWS and Azure public clouds, SaaS will include and/or incorporate cloud managed and packaged software services like Office Productivity, Analytics, Data Management, and Security.
- **IaaS:** Sourced via the AWS and Azure public clouds, PaaS will include and/or incorporate cloud platform services like Databases, Open Source services, and Development, Testing, and Deployment.
- **PaaS:** Sourced via the AWS and Azure public clouds, IaaS will include and/or incorporate cloud infrastructure services like Disaster Recovery, Operating Systems, Storage, Network, and Security.

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

Response:

For our proposed service models SaaS, IaaS, and PaaS, Presidio expresses its willingness to comply with the requirements of RFP Attachments C – NIST Service Models and D – Scope of Services. Our proposed cloud solutions adhere to the definitions specified in Attachment C. We will use the risk categories in Attachment D as a labeling system with regard to data and information systems. In general, the design of the public cloud solutions will incorporate security at all of the levels specified in the NASPO guidelines. Presidio's cloud vendors, AWS and Azure, will maintain the security of the cloud, whereas the Purchasing Entity/Presidio will be responsible for ensuring security best practices with regard to solution design and implementation.

8.1.3 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.

Response:

Presidio will adhere to the NIST Service Models and inherent definitions specified in RFP Attachment D – Scope of Services. The SaaS, PaaS, and IaaS models are distinct in our proposal.

Any hybrid offering is clearly defined using NIST-specified sub-categories with any exceptions identified, should they occur.

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.

Response:

Presidio is partnering with Amazon to provide any cloud solutions based on their AWS platform and with Microsoft to provide any cloud solutions based on their Azure platform.

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.

Response:

Presidio always attempts to utilize Presidio resources when delivering professional services to our customers; however, there may be occasions, due to a specific technology need or volume of services, when Presidio uses subcontractors to supplement our technology and professional services offerings in support of customer projects. We have developed relationships with a nationwide network of subcontractors with whom we have collaborated successfully on numerous projects in the past. When we use subcontractors in support of a project, Presidio, as the prime contractor, manages their performance to ensure subcontractors deliver the same level of customer satisfaction that Presidio is accustomed to providing. Presidio takes full responsibility for scheduling, coordinating, and managing subcontractors as if they are direct Presidio employees. Our goal is to provide a seamless face and a single point of contact to the Purchasing Entities.

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.

Response:

Since each state maintains different licensing, permits, and insurance requirements based on the category of work to be performed, specific subcontractors that will be engaged are unknown at this time. Our engineering and contract teams local to each region are responsible for vetting

subcontractors based on the Purchasing Entity's requirements. They ensure all state or local permitting, licensing, and insurance requirements are met before using a subcontractor.

Presidio leverages multiple contractors in each state but has the flexibility to partner with existing Purchasing Entity subcontractors. This allows Purchasing Entities to maintain existing in-state relationships and for Presidio to support the local economy. Presidio's regional contract and engineering teams can identify and rapidly on-board subcontractors within a short amount of time.

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.*

Response:

In performing its obligations under this agreement, Presidio will not have access to the Purchasing Entities' confidential information and systems, networks, and cloud infrastructure. Presidio acknowledges and understands that Purchasing Entities' protected assets contain data and information sensitive to the Purchasing Entities' business and its client's, and that Purchasing Entities are obligated legally and ethically to protect and maintain the security of such data and information. To the extent a security breach or incident occurs, Presidio's Contract Manager will use best efforts to assist Purchasing Entities with remediation efforts per the service guidelines expressly set forth in the Master Agreement but will not have any responsibility or liability for any damages, harm, loss, costs, or expenses incurred as a result, or in connection with such a security incident.

AWS

AWS services are content agnostic in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which customers store content. Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to place in the AWS cloud, only the customer can determine what level of security is appropriate for content stored and processed using AWS. Since customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches, and to notify regulators and affected individuals as required under applicable law.

AWS has implemented a formal, documented incident response policy and program. Developed in alignment with the ISO 27001 standard, this policy addresses purpose, scope, roles, responsibilities, and management commitment, and ensures system utilities are appropriately restricted and monitored. An outline of AWS's three-phased approach to managing incidents follows:

1) **Activation and Notification Phase**: Incidents for AWS begin with the detection of an event. This can come from several sources including:
   a) Metrics and alarms: AWS maintains an exceptional situational awareness capability; most issues are rapidly detected from 24x7x365 monitoring and alarming of real-time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
   b) Trouble ticket entered by an AWS employee.
   c) Calls to the 24X7X365 technical support hotline: If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g., Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.
2) **Recovery Phase:** The relevant resolvers will perform break fix to address the incident. After troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and actions, and end the call engagement.
3) **Reconstitution Phase:** After the relevant fix activities are complete, the call leader will declare that the recovery phase is complete. Post mortem and deep-root-cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions, such as design changes etc., will be captured in a Correction of Errors (COE) document and tracked to completion.

In addition to internal communication mechanisms, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

The AWS incident management program is reviewed by independent external auditors during audits for SOC, PCI DSS, ISO 27001, and FedRAMP compliance. Additionally, the AWS incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Plans are tested and updated through the due course of business (at least monthly).

Azure

Security is built into Microsoft Azure from the ground up, starting with the Security Development Lifecycle, a mandatory development process that incorporates privacy-by-design and privacy-by-default methodologies. The guiding principle of Microsoft's security strategy is to "assume breach," which is an extension of the defense-in-depth strategy. By constantly challenging the security capabilities of Azure, Microsoft can stay ahead of emerging threats.

Microsoft has a global, 24x7 incident response service that works to mitigate the effects of attacks against Microsoft Azure. Attested by multiple security and compliance audits (e.g., ISO/IEC 27018), Microsoft employs rigorous operations and processes at its data centers to prevent unauthorized access, including 24x7 video monitoring, trained security personnel, smart cards, and biometric controls.

The Microsoft Azure Security Response in the Cloud white paper further details how Microsoft investigates, manages, and responds to security incidents within Azure. The white paper is accessible via the following link: https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678.

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.

Response:

Unless otherwise authorized by the Participating Entity or the Master Agreement, Presidio will not permit its CSP partners to push adware, software, or marketing, and Presidio also will not engage in such activity.

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

Response:

AWS and Azure

Azure and AWS hosting environments can support any type of environment, including test/staging, production, pre-production, development, etc. These environments can also be isolated by utilizing separate Subscriptions dedicated to each type of environment for billing/chargeback clarity, and separation of services. These environments can then be seamlessly transitioned into a different environment stage with no to minimal downtime.

A summary for each service delivery model follows:

- **SaaS:** SaaS services on both the Azure and AWS platform have the ability to support different environment/deployment types depending on the hosted SaaS service. Certain services would require a separate "workspace" or portal to be deployed, while others will allow for multiple environments to exist in the same SaaS instance, but hosting environment types are still supported.

- **IaaS:** IaaS services for Azure/AWS are extremely flexible allowing for the configuration of any environment type. As an example - virtual networks, compute resources, storage resources, firewalls, etc. can all be deployed in separate subscriptions to help billing and logical separation between the environments, as well as providing clear delineation.
- **PaaS:** PaaS services in Azure/AWS are also flexible, with many offering multi-environment types within the same instance of the service. This allows for easy transition from an environment such as pre-production to production with little to no interruption. PaaS services can also be isolated by subscription.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

Response:

AWS

Applications and Web sites hosted on AWS are accessible to people with disabilities. The following compliance information is available for additional details:

AWS provides API-based cloud computing services with multiple interfaces to those services, including SDKs, IDE Toolkits, and Command Line Tools for developing and managing AWS resources. In addition, AWS provides two graphical user interfaces, the AWS Management Console and the AWS ElasticWolf Client Console.

The AWS ElasticWolf Client Console complies with Section 508 Standards requirements and AWS has prepared a Voluntary Product Accessibility Template (VPAT) for the Console, which outlines the Console's accessibility features. AWS will provide the VPAT upon request via the AWS Compliance website accessible via the following link: https://pages.awscloud.com/compliance-contact-us.html.

Azure

Microsoft is committed to ensuring products and services are designed for everyone, including the approximately 1.2 billion people with disabilities in the world. Accessibility makes it easier for people to see, hear, and use technology, and to personalize technology to meet their own needs and preferences.

Microsoft endeavors to integrate accessibility into every stage of product development, including planning, design, research, development, and testing. Microsoft's commitment is guided by three main principles:

- **Transparency**: Microsoft is open with its plans to ensure products are accessible. The Microsoft Accessibility website provides information about the accessibility of Microsoft products. Microsoft communicates openly about the accessibility of products and engages with stakeholders to resolve accessibility issues. Microsoft self-reports how products and services meet common accessibility requirements.

- **Inclusivity**: Microsoft wants everyone to be empowered—not only through its products, services, and technology, but within the culture at Microsoft. Microsoft's approach to inclusive design enables Microsoft to partner with individuals who have a range of abilities, and to share its learnings broadly so that other companies can benefit from them as well. Microsoft's Inclusive Design website offers resources such as videos, case studies, and an inclusive design toolkit.
- **Accountability**: Microsoft prioritizes inclusive design and accessibility in the development of all products and services by following established, company-wide standards. The Microsoft Accessibility Standards are company-wide guidelines that drive consideration for accessibility into every stage of production, including design, development, evaluation, and release of products and services.

The Microsoft Accessibility Standards support leading global accessibility standards, including:

- EN 301 549
- U.S. Section 508
- WCAG 2.0 (ISO/IEC 40500)

Microsoft also works with governments and organizations around the world to deliver the benefits of digital technology to people with disabilities. For example, Microsoft is a signatory to the Global Initiative for Inclusive Information and Communications Technology (G3ict) Charter, which encourages governments to increase digital inclusion for citizens by incorporating accessibility criteria into their procurement policies.

Microsoft in-scope services for EN 301 549 include:

- Azure and Azure Government
- Visual Studio Team Services
- Windows 10 Anniversary Update
- Windows Server 2016

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 a minimum.

Response:

AWS

Exhibit 6-2 details the web browsers supported by the AWS Management Console.

Exhibit 6-2. AWS Management Console Supported Web Browsers

Browser	Version
Google Chrome	Latest three versions
Mozilla Firefox	Latest three versions
Microsoft Edge	Latest three versions
Apple Safari for MacOS	Latest two versions
Microsoft Internet Explorer	11

Azure

Exhibit 6-3 details the web browsers supported by the Azure Portal.

Exhibit 6-3. Azure Portal Supported Web Browsers

Browser	Version
Google Chrome	Latest version
Mozilla Firefox	Latest version
Microsoft Edge	Latest version
Apple Safari for MacOS	Latest version, Mac only
Microsoft Internet Explorer	11

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.

Response:

Presidio conducts a discovery meeting with the Purchasing Entity to define workload requirements, process and controls of account creation, procurement of services, access management to portal, and procurement of selected services and service transition. From that meeting, a timeline will be discussed and addressed with the Purchasing Entity to ensure proper information is received and reviewed, and suggested services will be recommended.

Presidio does not require access to the customer's portal or to any data owned by the Purchasing Entity; therefore, specific compliance obligations with respect to any law, rule, or regulation concerning sensitive or personal information is the sole responsibility of the Purchasing Entity.

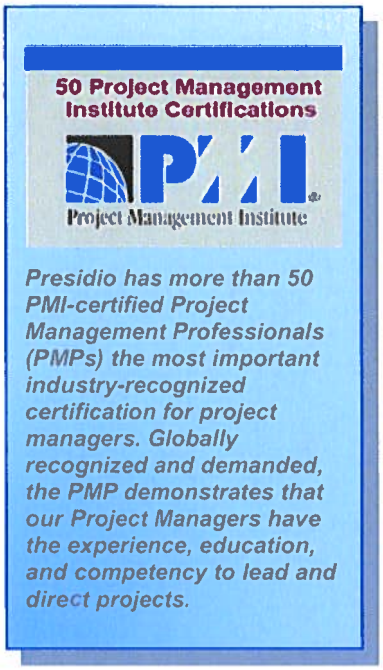
8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Response:

Presidio's project management methodology is based on the project management processes as defined in PMI's Project Management Body of Knowledge (PMBOK). These methods define a set of project management processes that we use as our project management approach to developing project plans, schedules, and work plans. Our process-based approach establishes reliable timelines for developing, testing, and implementing solutions for our clients. We create project schedules and work plans for each client tailored to their requirements, project scope, and overall solution.

Management Objectives and Priorities

PMBOK describes a broad model for project management activities. This model is adapted to the features of each particular project. The model facilitates the sharing of project management knowledge and experience, improves identification and usage of best practices, and improves project results by avoiding common pitfalls.



The key objective of our management approach is to develop a closed-loop process in which we establish and execute a plan, take measurements, and perform detailed analysis. The plan:

- Establishes schedules with sufficient milestones to measure progress in meaningful increments.
- Identifies the effort required to complete specific, well-defined tasks on the established schedule.
- Monitors the process for developing all deliverables to ensure quality is guaranteed throughout the entire process (e.g., we meet or exceed quality objectives).
- Provides a mechanism for orderly changes to be incorporated while understanding and agreeing to all impacts resulting from the change.
- Identifies existing and potential risks, and based on their significance and likelihood of occurring, determines alternatives to eliminate or mitigate them.

Measurable Project Milestones

We add project milestones after estimating the effort for the project activities and tasks. A milestone is either an activity that has zero duration or a specific deliverable that is due. Milestones provide an objective gauge of project progress. For example, the date that equipment is delivered to a site, received, and accepted or the date that the Risk Management Plan is to be submitted are both considered project milestones. Milestones are documented in and become a part of the Project Work Plan (PWP). The rollout strategy and schedule, including milestones, will be developed in conjunction with the Purchasing Entity's project team.

Project Work Plan

In formulating the PWP, Presidio will document exactly what must be done to complete a particular project. The Project Manager (PM) will facilitate a session with all project team members to establish PWP activities and tasks, and the effort involved to complete them is estimated. We then examine this draft to ensure a balance of hours and assigned resources, and to ensure it is consistent with the project scope. This will be done during the planning phase. When the PWP has been finalized by Presidio, it will be submitted to the Purchasing Entity for final approval prior to project implementation.

Project Tracking and Oversight

PWP management is the responsibility of the PM. Although project team members may sometimes update their assigned tasks, the PM has overall responsibility to ensure the PWP is up to date. The PM will review the plan to ensure the project is progressing as scheduled and assigned tasks are being completed by the dates set. After the PM's review and update, an updated PWP will be distributed to the appropriate personnel based upon the established Communication Plan.

Project Manager

Our Project Manager responsibilities typically include:

- Work with the Purchasing Entity and Presidio project personnel to prioritize and plan the activities for the duration of the engagement. Establish lines of communication and frequency of status reporting.
- Review and communicate the status of the project with periodic status reports or conference calls that highlight performance on planned tasks, as well as any issues or other areas requiring attention by Presidio and/or the Purchasing Entity.
- Monitor quality on the project and establish effective communications with the Purchasing Entity's staff, while maintaining focused, high-quality effort through project completion.
- Create an implementation schedule with all necessary tasks and associated timelines.
- Attend any appropriate Project Systems Engineering and Planning Phase Workshops that require PM participation and associated follow-up (Action Items, Resource Planning, etc.)
- Create project documentation artifacts, utilizing the client project governance procedures.
- Manage project budget, scope, schedule, and resources.
- Define and manage projects using PMI best practices.
- Conduct weekly variance analysis (e.g., effort, schedule, and budget)
- Actively and aggressively manage scope, issues, and risks.

- Develop and maintain product-based work breakdown structures (WBS) and project schedules.
- Work closely with the project sponsor on the business and technical objectives of the project.

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- *How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.*

Response:

As Presidio introduces or removes cloud solutions from its portfolio of offerings throughout the term of the Master Agreement, our dedicated Contract Manager will ensure:

- All new services will meet the minimum specifications, and terms and conditions outlined in the resulting master agreement and our proposal response.
- Any new additions with accompanying terms and conditions will not diminish or weaken existing terms and conditions.
- Presidio will adhere to the same pricing structure proposed for services in the equivalent service category and the same minimum discounts specified in our cost proposal will apply.
- Presidio will report any changes to its cloud offerings to the Lead State via updated Cloud Offerings Search Tool templates and pricing catalog.

- *How Offeror will maintain discounts at the levels set forth in the contract.*

Response:

Presidio will maintain its contractual obligation for discounts set forth in the contract with its customers. Any pricing discounts provided from our AWS and Azure cloud vendors are bound by the terms and conditions of our master cloud agreement and the commitments that the cloud vendors uphold by way of competitive subservices rates and resell pricing. Discounts for Professional Services are maintained throughout the contractual periods indicated in agreements between Presidio and its customers.

- *How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.*

Response:

When applicable, Presidio will present a proposal to the Purchasing Entity that introduces the technology changes and makes recommendations for services updates, explains the impact, and includes mitigation planning to address risks.

- *How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.*

Response:

Presidio will present a proposal to the Purchasing Entity that details operations support from its personnel, including professional services and any pertinent support and offerings from its Managed Services team as it relates to client operations. The support proposal will include relevant pricing information for services provided by Presidio along with strategic guidance on the change.

8.4 (E) CUSTOMER SERVICE

8.4.1 Offeror must describe how it will 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).*

Response:

Quality Assurance

Presidio recognizes the importance of Quality Management as a foundational business process. The Quality Management System (QMS) at Presidio is the primary responsibility of the Process and Quality Manager (PQM). The PQM is responsible for the measurement of Presidio processes. This includes operational processes, process, and procedures for estimating, requirements management, project planning/project monitoring and control, configuration management and overall analysis.

The PQM collaborates with Presidio's executive leadership to ensure the QMS aligns with corporate strategy, goals, and objectives. In addition to performing yearly surveillance audits and Management Reviews, the PQM also mentors Presidio employees and leads the cultural/behavioral initiative to ensure the successful delivery of engagements to anchor Presidio's position as an industry leader.

Effective Quality Management process is also a vehicle for meeting the needs of our customers. As such, Presidio is an **ISO 9001:2015** registered company.

- We address industry standards such as HIPAA, PCI, Sarbanes Oxley, NERC-CIP, FISMA and ISO 27001/2

As evidenced by our quality, process, and organizational certifications, Presidio provides a proven methodology for managing projects ensuring process effectiveness, oversight, and controls across our organization; this strengthens our ability to provide superior services and solutions to clients.

The following are Presidio's industry-recognized best-practice management, service, and delivery certifications:

Information Technology Infrastructure Library (ITIL) Best Practices

We employ more than 40 ITIL-certified individuals, including 20 ITIL V3 Foundation and 3 ITIL V3 Practitioner certifications.

Service Delivery Based on Project Management Institute

Presidio delivers superior services to clients consistently though our project and program management methodology based on PMI's Project Management Body of Knowledge (PMBOK).

Additionally, we have individuals who hold certifications in Lean Six Sigma Yellow Belt and our project management includes Project Management Institute (PMI)-certified Project Management Professionals (PMPs). Our mature, stable management approach and quality management system prove we consistently and reliably deliver what we promise.

International Organization for Standardization

ISO is an international standard for quality. This certification demonstrates and ensures Presidio takes seriously and provides industry-approved fundamental quality management processes designed to meet the needs of current and future customers. We were certified by the International Organization for Standardization's ISO 9001:2015 in April 2009. Presidio has fulfilled required reviews to ensure ongoing compliance with the applicable standards. Presidio was recertified in March 2015 with certification that is valid through April 2018.

Presidio's Relentless Pursuit of Customer Satisfaction

Presidio knows our existence depends on our customers. We participate in customer satisfaction initiatives with all of our key partners, and our culture fosters the highest levels of customer service. Our highly skilled and experienced team members share in this customer service philosophy of consistently meeting our clients' requirements and exceeding their expectations, resulting in over 95% staying with us year after year.

Presidio's strong commitment to client satisfaction is demonstrated by consistently high satisfaction ratings among our clients and leading vendor partners.

Presidio's Net Promoter Score Translates to Exceptional Client Experience

Net Promoter, is the worldwide standard for organizations to measure, understand, and improve their customer experience. Presidio has consistently maintained a Net Promoter Score above 50. Exhibit 6-4 illustrates Presidio's ranking on the Net Promoter Score Scale.

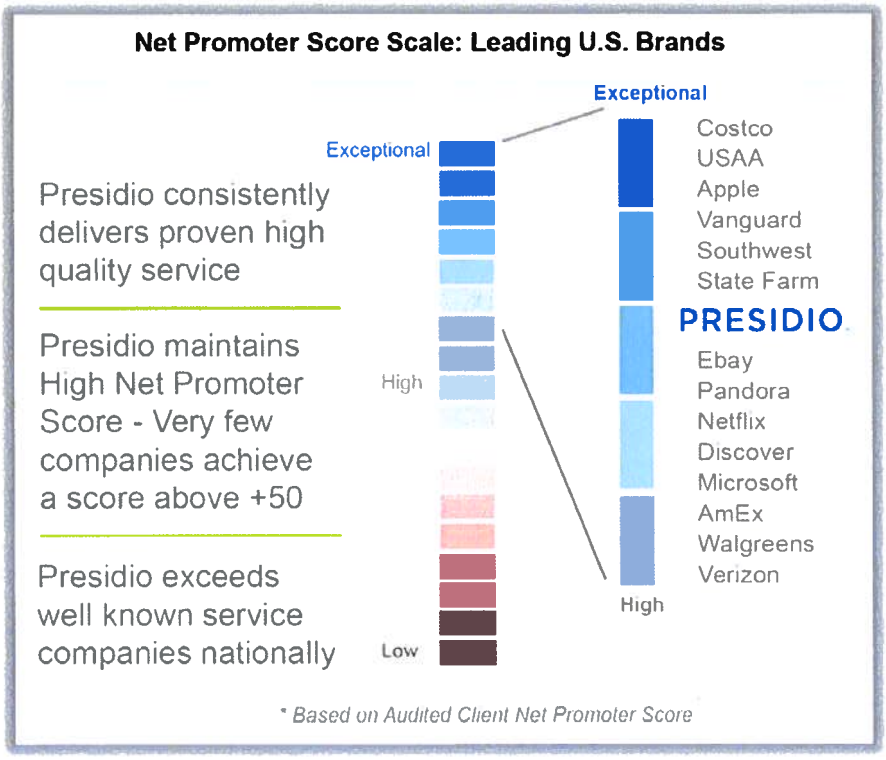


Exhibit 6-4. Presidio Net Promoter Score

Presidio consistently delivers proven high quality service.

Escalation Plan

In the unlikely event that the Purchasing Entities expectations are not being met and the Presidio Customer Service Representative cannot remedy the situation immediately, we will adhere to the internal escalation process detailed in Exhibit 6-5 to resolve any issues or concerns.

Exhibit 6-5. Presidio's Escalation Process

Level	Presidio Personnel	Allotted Response Time From Request
Level 1	Presidio Account Manager is notified of issue by Purchasing Entity	24 hours
Level 2	Presidio Sales Director/Manager	48 hours
Level 3	Presidio Regional Vice President	72 hours
Level 4	Presidio Area President	120 hours

Service Level Agreement

Please refer to the sample SLAs included in our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal.

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.

Response:

Presidio will assign a dedicated lead representative for each Purchasing Entity and will maintain current contact information for each representative. As we have done with other nationwide state contract vehicles, our Account Manager for each state will be designated as the lead representative.

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

Response:

With 60+ office locations across the United States, our lead representatives operate in all four North American time zones. As we have done with other nationwide state contract vehicles, our lead representatives will be available via email during the specified timeframe (local time) to ensure the Purchasing Entities receive the desired level of customer service.

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

Response:

Presidio's designated lead representative will respond to Purchasing Entity inquiries within 1 business day.

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

Response:

Presidio provides design services in support of all of the proposed cloud solutions. A summary for each service delivery model follows:

- **SaaS:** Presidio provides design services for Azure and AWS SaaS services. These services include native platform SaaS services, as well as third-party SaaS services and their integrations to the Azure and AWS platforms.
- **IaaS:** Presidio provides design services for Azure and AWS IaaS services to include hybrid connectivity, platform-specific networking, compute, storage, backup and recovery, and many different IaaS components throughout the design process.

- **PaaS:** Presidio provides design services for Azure and AWS PaaS services such as SQL Data Warehouse, Azure Site Recovery, Azure Automation, Logic Apps, Functions, and many other PaaS services offered by both providers.

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

Response:

Presidio provides installation services in support of all of the proposed cloud solutions. A summary for each service delivery model follows:

- **SaaS:** Presidio provides post-design/delivery services for the deployment, installation, and configuration of native and third-party SaaS services on both AWS and Azure.
- **IaaS:** Presidio provides post-design/delivery services for the deployment, installation, and configuration of IaaS networking/compute/storage resources on both AWS and Azure. This also includes data center connectivity and multi-cloud connectivity services, as well as migration services.
- **PaaS:** Presidio provides post-design/delivery services for the deployment, installation, and configuration of AWS and Azure PaaS services, such as SQL Data Warehouse, Azure SQL Database, Logic Apps, Functions and more. This also includes migration services from traditional infrastructure to PaaS services.

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.

Response:

AWS and Azure

Cloud vendors are obligated to carry out all customer requests for deletion of data, including requests that are accidental or malicious. Presidio minimizes the risk of user-driven data loss by electing data recovery options within the SaaS, IaaS, PaaS, or hybrid solutions. Elements of the design that facilitate this are secure data backup solutions, active replication, and complete restore options to meet RPO/RTO objectives. Ring layer security for data is used as a design principle to encrypt data at rest and in motion. Data that is infrequently accessed (IA) is moved to appropriate IA via scripts or automated rules, and archived on long-term storage defined by client data retention needs. In addition, data disposal is supported for secure deletion by authorized personnel or authenticated applications based on Role-Based Access Controls (RBAC).

Presidio Managed Services

Information resources are some of the most valuable assets of Presidio Managed Services, and, as is the case with all valuable assets, they need to be protected accordingly. The meaning of "accordingly" is driven by legal, financial, and operational requirements and is based on the criticality and risk level of the information. To help protect information resources appropriately, each information resource produced or handled by Presidio Managed Services is assigned one of three classifications based on the level of protection required for that resource.

In increasing order of protection level, the classifications used by Presidio Managed Services are Unrestricted, Restricted, and Confidential. Information that is owned by a third party/client/customer but managed by Presidio Managed Services will use one of the classification levels but with the addition of the "Third Party" addendum.

Unrestricted

Unrestricted is information that can be disclosed to any person inside or outside Presidio Managed Services, as this disclosure causes no harm. Although security controls are not needed to prevent disclosure and dissemination of this information, they are still necessary to protect against unauthorized modification, destruction, or loss of the information.

Examples of Unrestricted information include:

- Personnel information designated as public such as:
  - Employee name,
  - E-mail addresses,
  - Job/Position title,
  - Office mailing address,
  - Office telephone number,
  - Office email address,
  - Marketing brochures, and
  - Service catalogs and schedules.

Restricted

Restricted is information that is generally not public, and whose disclosure, loss, or corruption may cause a significant short-term impact on operations of tactical objectives of Presidio Managed Services. The information requires protection against unauthorized access and disclosure, modification, destruction, and use.

Examples of Restricted Information include:

- Personnel information designated as private such as:
  - Employee personal number,
  - Employee date and place of birth,

- Employee home address,
- Employee annual review,
- Employee resumes,
- Employee salary and benefit data,
- Internal correspondence and minutes from meetings,
- Invoices and internal billing,
- Detailed annual budget information,
- Internal Standard Operating Procedures,
- Social Security number,
- Driver's license number,
- Protected Health Information (PHI),
- Personally Identifiable Information (PII), and
- Human Resources (HR) data to include applicants.

Confidential

Confidential is information that is generally not public, and whose disclosure, loss, or corruption may cause serious impact on long-term strategic objects and/or puts the survival of Presidio Managed Services at risk. The information requires protection against unauthorized access and disclosure, modification, destruction, and use.

Examples of Confidential Information include:

- Specific Presidio Managed Services infrastructure information such as:
  - Specific resource names,
  - Network mapping,
  - Financial account numbers,
  - Passwords,
  - IP addresses, and
  - Any information related to Presidio Managed Services operations.

The classification level determines the information security controls that must be applied to protect an information resource, and the procedures that must be followed when acquiring, storing, using, transmitting, archiving, and destroying that resource.

Examples of the handling of Information are as follows:

- Providing (restricting) access to information.
- Labeling information.

- Storing electronic information (Data at Rest).
- Storing printed information.
- Printing information.
- Transmitting information (Data in Transit).
- Using classified information (Data in Use).
- Archiving information (record retention).
- Disposing of (destroying) information.

Information will be protected based on classification through any of the above means from beginning to end. If copies are made, they will be protected at the same level as the original.

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

Response:

AWS and Azure

Presidio intends to be fully compliant with data privacy and security by providing transparency of the ownership and control of customer content as follows:

- **Access:** Customers manage access to content, and user access to cloud services and resources. The cloud vendors provide an advanced set of access, encryption, and logging features to help customers do this effectively. AWS, Azure, and Presidio will not access or use customer content for any purpose without their consent. We never use content or derive information from it for marketing or advertising.
- **Storage**: Customers can choose the region(s) in which content is stored. We do not move or replicate content outside of a customer's chosen region(s) without their consent.
- **Security**: Customers choose how the content is secured. AWS and Azure offer customers strong encryption for their content in transit and at rest, and provide customers with the option to manage their own encryption keys.
- **Disclosure of customer content:** AWS and Azure do not disclose customer content unless they are required to do so to comply with the law, or with a valid and binding order of a governmental or regulatory body. Unless cloud vendors are prohibited from doing so or there is clear indication of illegal conduct in connection with the use of their products or services, they notify customers before disclosing customer content so they can seek protection from disclosure.
- **Security Assurance:** AWS and Azure have developed security assurance programs that uses best practices for global privacy and data protection to help customers operate securely within the public cloud, and to make the best use of the security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

Presidio Managed Services

Presidio Managed Services' information system may generate audit records based on the following subjects: User authentication, System access, System Configuration Change, Audit Circumvention, System initialization, Program installation, Account modification, and/or the transfer of information out of the system. These events are necessary to support after-the-fact investigations of security incidents and will be reviewed and updated periodically.

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.

Response:

AWS

AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Azure

Microsoft business cloud services take strong measures to help protect customer data from inappropriate access or use by unauthorized persons. This includes restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data. However, customers can access their own customer data at any time and for any reason. During the term of the customer's subscription to Microsoft business services, the customer can access and extract its customer data. Customers of Azure, Dynamics 365, Intune, and Office 365 in-scope services can retrieve a copy of their customer data at any time and for any reason without the need to notify Microsoft or ask for assistance. Also, customers can take their customer data with them if they end their subscription. Microsoft takes strong measures to help protect customer data from inappropriate access or use by unauthorized persons, either external or internal, and to prevent customers from gaining access to one another's data.

The operational processes that govern access to customer data in Microsoft business cloud services are protected by strong controls and authentication, which fall into two categories: physical and logical.

Access to physical datacenter facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations center.

Virtual access to customer data is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

In addition, Microsoft uses encryption to safeguard customer data and help customers maintain control over it. When data moves over a network—between user devices and Microsoft datacenters or within datacenters themselves—Microsoft products and services use industry-standard secure transport protocols. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities.

Most Microsoft business cloud services are multitenant services, meaning that customer data, deployments, and virtual machines may be stored on the same physical hardware as that of other customers. Microsoft uses logical isolation to segregate storage and processing for different customers through specialized technology engineered to help ensure a customer's data is not combined with anyone else's.

Business cloud services with audited certifications such as ISO 27001 are regularly verified by Microsoft and accredited audit firms, which perform sample audits to attest that access is only for legitimate business purposes.

Microsoft operations and support personnel are located around the globe to help ensure appropriate personnel are available 24 hours a day, 365 days a year. Microsoft has automated a majority of its service operations so that only a small set requires human interaction.

Microsoft engineers do not have default access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary.

Microsoft personnel will use customer data only for purposes compatible with providing the contracted services, such as troubleshooting and improving features, such as protection from malware.

Microsoft's enterprise online services process various categories of data, including customer data, support data, and personal data. Where Microsoft hires a subcontractor to perform work that may require access to such data, they are considered a subprocessor.

Many of the subprocessors provide contract staff that work alongside Microsoft employees to help deliver the services. In such cases, the data is processed solely in Microsoft facilities, on Microsoft systems, and always subject to Microsoft policies and supervision.

Subprocessors may access data only to deliver the services Microsoft has hired them to provide and are prohibited from using data for any other purpose. They are required to maintain the confidentiality of this data and are contractually obligated to meet strict privacy requirements that are equivalent to or stronger than the contractual commitments Microsoft makes to its customers. Subprocessors are also required to meet EU General Data Protection Regulation requirements, including those related to employing appropriate technical and organizational measures to protect personal data.

Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardize and strengthen the handling of data, and to ensure supplier business processes and systems are consistent with those of Microsoft.

Subprocessors who handle customer data (including personal data therein) are subject to heightened requirements. Subprocessors of customer data must agree to the EU Model Clauses for services for which Microsoft offers its customers the EU Model Clauses.

In the case of government surveillance, Microsoft has taken steps to ensure there are no "back doors" and no direct or unfettered government access to customer data. Microsoft imposes carefully defined requirements for government and law enforcement requests for customer data.

Microsoft will not disclose data hosted in Microsoft business services to a government agency unless required by law. If Microsoft is compelled by law to disclose customer data, Microsoft will promptly notify the customer and provide a copy of the request, unless Microsoft is legally prohibited from doing so.

Presidio Managed Services

Presidio Managed Services' policy states that systems, user accounts, or user data is only accessed during the course of delivering services. This policy further defines that access is controlled and secured. The Presidio Managed Services' information system will display a notification message before granting system access informing potential users of the following:

- User is accessing information system.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

Presidio Managed Services' system use of notification messages will be implemented in the form of warning banners displayed when individuals log in to the information system. This will include appropriate privacy and security notices, and will remain on the screen until the user takes explicit actions to log on to the information system.

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.

Response:

Please refer to our previous response to RFP section 6.5.3 in the document entitled, "Presidio Business Information.pdf" uploaded in response to #2.1.5 in the SciQuest portal.

Presidio readily acknowledges and supports the NIST definitions for cloud computing. This includes the service models (i.e., SaaS, PaaS, and IaaS) as well as the deployment models (i.e., private cloud, community cloud, public cloud, and hybrid cloud).

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.

Response:

AWS

AWS Compliance enables customers to understand the robust controls in place at AWS that facilitate security and data protection in the cloud. The AWS Cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices, including:

- Federal Risk and Authorization Management Program (FedRAMP).
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3.
- Payment Card Industry Data Security Standard (PCI DSS).
- International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001.
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6.
- Federal Information Security Management Act (FISMA).
- US Health Insurance Portability and Accountability Act (HIPAA).
- FBI Criminal Justice Information Services (CJIS).
- National Institute of Standards and Technology (NIST) 800-171.
- International Traffic in Arms Regulations (ITAR).
- Federal Information Processing Standard (FIPS) 140-2.
- Family Educational Rights and Privacy Act (FERPA).
- Information Security Registered Assessors Program (IRAP) (Australia).
- IT-Grundschutz (Germany).

For information on all of the security regulations and standards with which AWS complies, please refer to the AWS Compliance page accessible via the following link: https://aws.amazon.com/compliance/.

Azure

Microsoft leads the industry in establishing clear security and privacy requirements, and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. Additional information is accessible via the following link: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942.

Presidio Managed Services

Presidio Managed Services maintains the SOC 2 Type 2 for our overall services environment. PCI DSS for an isolated, segregated environment to support Cardholder Data Environments (CDE). Documentation can be provided annually and/or on demand.

Presidio Managed Services is aligning to the ISO 27001/2 with a certification goal of August 2019. NIST 800-53, NIST SP 800-171, and FIPS 200 are utilized as references towards this initiative.

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.

Response:

AWS

AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used to support communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during weekly operations meetings.

AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region and additional capacity protect against the possibility of DoS attacks.

The AWS network provides significant protection against traditional network security issues, and clients can also implement further protection. Following are a few examples:

- **Distributed Denial of Service (DDoS) Attacks**: AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks**: All of the AWS APIs are available via SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. Clients can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. AWS encourages clients to use SSL for all interactions with AWS.
- **IP Spoofing**: Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**: Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on AWS's website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by clients. A client's strict management of security groups can further mitigate the threat of port scans. If clients configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, the client must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. A client may request permission to conduct vulnerability scans as required to meet specific compliance requirements. These scans must be limited to a client's own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at the following link: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest.

- **Packet sniffing by other tenants**: It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While clients can place interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice clients should encrypt sensitive traffic.

Azure

Threat management includes protection from both malicious software and attacks against systems and networks. Microsoft products and services have built-in protection features to help defend your data against malware and other types of threats.

Microsoft cloud services help you protect against malware threats in multiple ways. Microsoft Antimalware is built for the cloud, and additional antimalware protections are provided in specific services. Denial-of-service (DoS) attacks can deny access to important resources and result in lost productivity, so Microsoft builds its services to defend against such attacks. Windows server and client operating systems include multiple technologies for protecting against these threats at the local level.

Security Technologies

Microsoft uses many security technologies and practices to protect the cloud infrastructure and on-premises networks against modern, sophisticated threats:

- Antimalware components and services for cloud services, virtual machines (VMs), and Windows clients and servers help identify and remove viruses, spyware, and other malicious software. Antimalware also provides real-time protection, on-demand scanning, basic configuration management, and monitoring. Microsoft Antimalware for Azure cloud services and virtual machines is built on the same antimalware platform as other Microsoft malware protection products, and provides a single-agent solution for applications and tenant environments.
- Distributed denial-of-service defenses protect Microsoft's cloud services from network-layer high-volume attacks that choke network pipes and packet-processing capabilities by flooding the network with packets. Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the Azure continuous monitoring and penetration-testing processes. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. The Azure DDoS defense technology provides detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to help ensure network-layer high-volume attacks on the platform itself do not impact customer environments. Application-layer attacks, on the other hand, are direct attacks launched against a customer deployment. The Azure DDoS defense system does not provide mitigation or actively block network traffic affecting

individual customer deployments, as it is not possible for the system to interpret the expected behavior of customer applications.

- Advanced Threat Analytics is technology that monitors normal usage patterns for networks, systems, and users, and employs machine learning to flag any behavior that is out of the ordinary. Advanced Threat Analytics uses information derived from networked devices and heuristics to detect suspicious activity that may indicate a threat; it then sends real-time alerts so that customers can mount a response to protect their assets.

Microsoft threat management technologies were developed based on Microsoft's experience addressing emerging threats in the public cloud, private cloud, and data center environments, and are driven by the "assume breach" approach.

Threat management processes are designed to adapt quickly to the changing threat landscape. Highly specialized groups of security experts, known as the Red Team, use their expertise to strengthen threat detection, response, and defense for Microsoft enterprise cloud services. They simulate real-world breaches, conduct continuous security monitoring, and practice security incident response to validate and improve the security of the services.

Microsoft Antimalware for Azure cloud services and virtual machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. Customers can configure alerts to inform them when known malicious or unwanted software attempts to install itself or run on their Azure systems. When malware is detected, Antimalware automatically responds by acting to delete or quarantine malicious files and clean up malicious registry entries.

- **Distributed denial-of-service defenses**: To protect its cloud services, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the Azure continuous monitoring and penetration-testing processes. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks.
- **Threat management partners**: In addition to the robust security benefits built into Azure, Microsoft offers a rich array of additional security products for Azure that are built to meet customers' unique security needs.
- **Azure Security Center (Security Center)** provides a centralized portal from which customers can secure their Azure deployments, and prevent, detect, respond to threats, and increase visibility into the security of Azure resources. Security Center also provides focused security recommendations and rapid deployment of integrated partner technologies. It uses behavioral analytics and machine learning for effective threat detection and helps customers build an attack timeline for faster remediation.

Presidio Managed Services

Presidio Managed Services has a robust policy to manage, maintain, and administrate access control. Access control ensures the proper rights are provided to authorized users and keeps the information assets secure.

The following policy formalizes the procedures to implement the identification and authentication policy to include the associated identification and authentication controls.

User Identification and Authentication

Each user shall have a unique identifier (user ID) and associated password for his/her use only. Shared accounts are documented in ServiceNow.

All passwords must be unique and known only by the user to whose account it is assigned. Initial passwords for newly-created accounts and reset passwords must also be unique and must be changed immediately by the user upon first use. A password must be changed immediately if known or thought to be compromised or non-compliant with this policy.

Device Identification and Authentication

Presidio Managed Services information systems will identify and authenticate devices before establishing a connection. Systems use shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) and/or an authenticated encrypted solution (e.g., Virtual Private Network (VPN)) to identify and authenticate devices on the local networks.

Identifier Management

Presidio Managed Services will manage user identifiers through the following means:

- Uniquely identifying each user.
- Verifying the identity of each user.
- Receiving authorization to issue a user identifier from an appropriate official.
- Issuing the user identifier to the intended party.
- Disabling the user identifier after 30 days of inactivity.
- Archiving user identifiers.

Authentication Management

Presidio Managed Services will protect passwords from unauthorized disclosure and modification when stored and transmitted via the PMS Password Policy, which includes:

- Prohibiting passwords from being displayed when entered.
- Enforcing password minimum and maximum lifetime restrictions.
- Prohibits password reuse for a specified number of generations.

Access Control Policy and Procedures

Presidio Managed Services will develop, disseminate, and review and update this access control policy periodically to address purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance, which formalizes documented procedures to facilitate the implementation of this access control policy and associated controls.

Account Management

Presidio Managed Services will manage system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Presidio Managed Services will review system accounts semi-annually to include the following:

- Identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations.
- Authorized users of the information system and specify access rights/privileges.
- Grant access to its information system based on a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage.
- Require proper identification for requests to establish information system accounts and approve all such requests.
- Authorize and monitor the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts.
- Notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.
- Managers will be notified when users' information system usage or need-to-know/need-to-share changes.
- Use the following control elements to manage accounts:
    1. Automated support of the management of system accounts i.e., LastPass.
    2. Automatically terminate temporary and emergency accounts after 30 days.
    3. Automatically disable inactive accounts after 30 days.
    4. Automated audits for account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

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).

Response:

AWS

AWS does not access customer data, and customers are given the choice as to how they store, manage, and protect their data.

Azure

Processing of Customer Data; Ownership

Customer data will be used or otherwise processed only to provide customer the Online Services including purposes compatible with providing those services. Microsoft will not use or otherwise process customer data or derive information from it for any advertising or similar commercial purposes. As between the parties, customer retains all right, title, and interest in, and to, customer data. Microsoft acquires no rights in customer data, other than the rights customer grants to Microsoft to provide the Online Services to customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to customer.

Disclosure of Customer Data

Microsoft will not disclose customer data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as customer directs, (2) as described in the OST, or (3) as required by law.

Microsoft will not disclose customer data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for customer data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from customer. If compelled to disclose customer data to law enforcement, Microsoft will promptly notify customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for customer data, Microsoft will promptly notify customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to customer data; (b) platform encryption keys used to secure customer data or the ability to break such encryption; or (c) access to customer data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide customer's basic contact information to the third party.

Processing of Personal Data; GDPR

Personal data provided to Microsoft by, or on behalf of, customer through use of the Online Service is also customer data. Pseudonymized identifiers may also be generated through customer's use of the Online Services and are also personal data.

Presidio Managed Services

To help protect information resources appropriately, each information resource produced or handled by Presidio Managed Services is assigned one of three classifications based on the level of protection required for that resource.

In increasing order of protection level, the classifications used by Presidio Managed Services are Unrestricted, Restricted, and Confidential. Information that is owned by a third party/client/customer but managed by Presidio Managed Services will use one of the classification levels but with the addition of the "Third Party" addendum. Please refer to our previous response to #8.5.1 in this section for information on the classification levels and handling of classified information.

Third-party Addendum

Third-party addendum classification will be added to one of the three classifications if the information being classified is owned by a third party and only managed by Presidio Managed Services. An example of a third-party addendum would be the password files of a client/customer, which would be classified as Third-Party Confidential.

Assigning Classification Levels

Information owners are responsible for assigning the appropriate classification to each information resource for which they are responsible, and ensuring that the resource is protected in accordance with that classification.

Many information resources will not be explicitly classified, particularly if they are not in the form of a printed or electronic document. Information that is not explicitly classified is classified as Confidential.

Labelling of Information

Labelling of Unrestricted information is not required. However, if in doubt, the classification will be considered to be Confidential until further investigation of the information can be completed. In addition, information not specifically labeled and not unrestricted will be considered to be Confidential.

When assigning a classification to data, it will be labeled as follows:

- Classification will be in the footnote of the document.
- Classification will be preceded by the entity classifying the information i.e., Presidio Managed Services, Third Party, etc.

Please refer to our preceding response to #8.6.3 in this section for information on Presidio's account management policies and procedures.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Response:

AWS

Please refer to our previous response to #8.6.2 in this section. For information on all of the security regulations and standards with which AWS complies, please refer to the AWS Compliance page accessible via the following link: https://aws.amazon.com/compliance/.

Azure

Please refer to the Microsoft Azure Compliance information accessible via the following link: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942.

Presidio Managed Services

Currently, Presidio Managed Services is not FedRAMP certified; however, we will work with our cloud partners to ensure only FedRAMP environments are provided for this contract.

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.

Response:

AWS

The logging and monitoring of Application Program Interface (API) calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS customers can leverage multiple AWS features and capabilities, along with third-party tools, to monitor their instances and manage/analyze log files.

AWS CloudTrail

AWS CloudTrail is a web service that records API calls to supported AWS services in an AWS account, delivering a log file to an Amazon Simple Storage Service (Amazon S3) bucket. AWS CloudTrail alleviates common challenges experienced in an on-premise environment by making it easier for customers to enhance security and operational processes while demonstrating compliance with policies or regulatory standards.

With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

For information on the services and features supported by AWS CloudTrail, visit the AWS CloudTrail FAQs on the AWS website accessible via the following link: https://aws.amazon.com/cloudtrail/faqs/.

The AWS whitepaper, "*Security at Scale: Logging In AWS,*" provides an overview of common compliance requirements related to logging, detailing how AWS CloudTrail features can help satisfy these requirements. This whitepaper is accessible via the following link: https://aws.amazon.com/cloudtrail/faqs/.

The AWS whitepaper, "*Auditing Security Checklist for Use of AWS,*" provides customers with a checklist to assist in evaluating AWS for the purposes of an internal review or external audit. This whitepaper is accessible via the following link: http://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf.

AWS CloudTrail: Features and Benefits

Some of the key features of AWS CloudTrail include:

- **Increased Visibility**: AWS CloudTrail provides increased visibility into user activity by recording AWS API calls. Customers can answer questions such as, what actions did a given user take over a given time period? For a given resource, which user has taken actions on it over a given time period? What is the source IP address of a given activity? Which activities failed due to inadequate permissions?
- **Durable and Inexpensive Log File Storage**: AWS CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably and inexpensively. Customers can use Amazon S3 lifecycle configuration rules to further reduce storage costs. For example, customers can define rules to automatically delete old log files or archive them to Amazon Glacier for additional savings.
- **Easy Administration:** AWS CloudTrail is a fully managed service; customers simply turn on AWS CloudTrail for their account using the AWS Management Console, the Command Line Interface, or the AWS CloudTrail SDK and start receiving AWS CloudTrail log files in the specified Amazon S3 bucket.
- **Notifications for Log File Delivery**: AWS CloudTrail can be configured to publish a notification for each log file delivered, thus enabling customers to automatically take action upon log file delivery. AWS CloudTrail uses the Amazon Simple Notification Service (Amazon SNS) for notifications.
- **Choice of Partner Solutions**: Multiple partners, including AlertLogic, Boundary, Loggly, Splunk, and Sumologic, offer integrated solutions to analyze AWS CloudTrail log files. These solutions include features like change tracking, troubleshooting, and security analysis. For more information, please refer to the AWS CloudTrail partners section accessible via the following link: https://aws.amazon.com/cloudtrail/partners/.
- **Log File Aggregation**: AWS CloudTrail can be configured to aggregate log files across multiple accounts and regions so that log files are delivered to a single bucket. For detailed instructions, refer to the Aggregating CloudTrail Log Files to a Single Amazon

S3 Bucket section of the user guide accessible via the following link: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-log-files-from-multiple-regions.html.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by customer applications and services, and any log files that applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep their application running smoothly.

Customers can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Customers can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

LogAnalyzer for Amazon CloudFront

LogAnalyzer allows customers to analyze their Amazon CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application customers can generate usage reports containing total traffic volume, object popularity, a breakdown of traffic by client IPs, and edge location. Reports are formatted as tab delimited text files, and delivered to the Amazon S3 bucket that customers specify.

Amazon CloudFront's Access Logs provide detailed information about requests made for content delivered through Amazon CloudFront, AWS's content delivery service. The LogAnalyzer for Amazon CloudFront analyzes the service's raw log files to produce a series of reports that answer business questions commonly asked by content owners.

Reports Generated

This LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs: 1) Overall Volume Report, 2) Object Popularity Report, 3) Client IP Report, and 4) Edge Location Report. The Overall Volume Report displays total amount of traffic delivered by CloudFront over the course of whatever period specified. The Object Popularity Report shows how many times each customer object is requested. The Client IP Report shows the traffic from each different Client IP that made a request for content. The Edge Location Report shows the total number of traffic delivered through each edge location. Each report measures traffic in three ways: the total number of requests, the total number of bytes transferred, and the number of request broken down by HTTP response code. The LogAnalyzer is implemented using Cascading (http://www.cascading.org) and is an example of how to construct an Amazon Elastic MapReduce application. Customers can also customize reports generated by the LogAnalyzer.

Third-Party Tools

Many third-party log monitoring and analysis tools are available on AWS Marketplace Accessible via the following link: https://aws.amazon.com/marketplace.

Azure

Auditing and logging of security-related events, and related alerts, are important components in an effective data protection strategy. Security logs and reports provide an electronic record of suspicious activities and help customers detect patterns that may indicate attempted or successful external penetration of the network, as well as internal attacks. Customers can use auditing to monitor user activity, document regulatory compliance, perform forensic analysis, and more. Alerts provide immediate notification when security events occur.

Microsoft Azure services and products provide configurable security auditing and logging options to help identify gaps in security policies and mechanisms, and address those gaps to help prevent breaches. Microsoft services offer some (and in some cases, all) of the following options: centralized monitoring, logging, and analysis systems to provide continuous visibility; timely alerts; and reports to help manage the large amount of information generated by devices and services.

Microsoft Azure log data can be exported to Security Incident and Event Management (SIEM) systems for analysis and integrates with third-party auditing solutions.

Types of Logs in Azure

Cloud applications are complex with many moving parts. Logs provide data to ensure customers' applications stay up and running in a healthy state. It also helps customers to stave off potential problems or troubleshoot past ones. In addition, customers can use logging data to gain deep insights about their applications. That knowledge can help customers to improve application performance or maintainability, or automate actions that would otherwise require manual intervention.

Azure produces extensive logging for every Azure service. These logs are categorized by these main types:

- Control/management logs give visibility into the Azure Resource Manager CREATE, UPDATE, and DELETE operations. Azure Activity Logs is an example of this type of log.
- Data plane logs give visibility into the events raised as part of the usage of an Azure resource. Examples of this type of log are the Windows event System, Security, and Application logs in a virtual machine and the Diagnostics Logs configured through Azure Monitor.
- Processed events give information about analyzed events/alerts that have been processed on a customer's behalf. Examples of this type are Azure Security Center Alerts where Azure Security Center has processed and analyzed their subscription and provides concise security alerts.

Activity Log

The Azure Activity Log provides insight into the operations that were performed on resources in a subscription. The Activity Log was previously known as "Audit Logs" or "Operational Logs," since it reports control-plane events for subscriptions. Using the Activity Log, customers can determine the "what, who, and when" for any write operations (PUT, POST, DELETE) taken on the resources in their subscription. Customers can also understand the status of the operation and other relevant properties. The Activity Log does not include read (GET) operations.

Here PUT, POST, DELETE refers to all the write operations activity log contains on the resources. For example, customers can use the activity logs to find an error when troubleshooting or to monitor how a user in the organization modified a resource.

Customers can retrieve events from Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API. Activity logs have a 19-day data retention period.

Integration scenarios include:

- Create an email or webhook alert that triggers off an Activity Log event.
- Stream it to an Event Hub for ingestion by a third-party service or custom analytics solution such as PowerBI.
- Analyze it in PowerBI using the PowerBI content pack.
- Save it to a Storage Account for archival or manual inspection. Customers can specify the retention time (in days) using Log Profiles.
- Query and view it in the Azure portal.
- Query it via PowerShell Cmdlet, CLI, or REST API.
- Export the Activity Log with Log Profiles to log Analytics.

Customers can use a storage account or event hub namespace that is not in the same subscription as the one emitting log. The user who configures the setting must have the appropriate RBAC access to both subscriptions

Azure Diagnostic Logs

Azure Diagnostic Logs are emitted by a resource that provides rich, frequent data about the operation of that resource. The content of these logs varies by resource type (e.g., Windows event system logs are one category of Diagnostic Log for VMs and blob, table, and queue logs are categories of Diagnostic Logs for storage accounts) and differ from the Activity Log, which provides insight into the operations that were performed on resources in the subscription.

Azure Diagnostics logs offer multiple configuration options using PowerShell, Command-line interface (CLI), and REST API.

Integration scenarios include:

- Save them to a Storage Account for auditing or manual inspection. Customers can specify the retention time (in days) using the Diagnostic Settings.

- Stream them to Event Hubs for ingestion by a third-party service or custom analytics solution such as PowerBI.
- Analyze them with Log Analytics.

Azure Active Directory Reporting

Azure Active Directory (Azure AD) includes security, activity, and audit reports for a customer's directory. The Azure Active Directory Audit Report helps customers to identify privileged actions that occurred in their Azure Active Directory. Privileged actions include elevation changes (e.g., role creation or password resets), changing policy configurations (e.g., password policies), or changes to directory configuration (e.g., changes to domain federation settings).

The reports provide the audit record for the event name, the actor who performed the action, the target resource affected by the change, and the date and time (in UTC). Customers are able to retrieve the list of audit events for their Azure Active Directory via the Azure portal.

The data of these reports can be useful to customer applications, such as SIEM systems, audit, and business intelligence tools. The Azure AD reporting APIs provide programmatic access to the data through a set of REST-based APIs. Customers can call these APIs from various programming languages and tools.

Events in the Azure AD Audit report are retained for 180 days.

Storage Analytics

Azure Storage Analytics performs logging and provides metrics data for a storage account. Customers can use this data to trace requests, analyze usage trends, and diagnose issues with their storage account. Storage Analytics logging is available for the Blob, Queue, and Table services. Storage Analytics logs detailed information about successful and failed requests to a storage service.

This information can be used to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis. Log entries are created only if there are requests made against the service endpoint. For example, if a storage account has activity in its Blob endpoint but not in its Table or Queue endpoints, only logs pertaining to the Blob service are created.

To use Storage Analytics, customers must enable it individually for each service they want to monitor. Customers can enable it in the Azure portal and c can also enable Storage Analytics programmatically via the REST API or the client library. Use the Set Service Properties operation to enable Storage Analytics individually for each service.

The aggregated data is stored in a well-known blob (for logging) and in well-known tables (for metrics), which may be accessed using the Blob service and Table service APIs.

Storage Analytics has a 20-TB limit on the amount of stored data that is independent of the total limit for a storage account. All logs are stored in block blobs in a container named $logs, which are automatically created when Storage Analytics is enabled for a storage account.

Azure Networking Logs

Network logging and monitoring in Azure is comprehensive and covers two broad categories:

- Network Watcher: Scenario-based network monitoring is provided with the features in Network Watcher. This service includes packet capture, next hop, IP flow verify, security group view, and NSG flow logs. Scenario level monitoring provides an end-to-end view of network resources in contrast to individual network resource monitoring.
- Resource monitoring: Resource level monitoring comprises of four features: diagnostic logs, metrics, troubleshooting, and resource health. All of these features are built at the network resource level.

Network Watcher is a regional service that enables customers to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Network diagnostic and visualization tools available with Network Watcher help customers understand, diagnose, and gain insights to their network in Azure.

Network Security Group Flow Logging

Network Security Group flow logs are a feature of Network Watcher that allows customers to view information about ingress and egress IP traffic through a Network Security Group. These flow logs are written in JSON format and show outbound and inbound flows on a per rule basis, the NIC the flow applies to, 5-tuple information about the flow (Source/Destination IP, Source/Destination Port, Protocol), and if the traffic was allowed or denied.

While flow logs target Network Security Groups, they are not displayed the same as the other logs. Flow logs are stored only within a storage account.

The same retention policies as seen on other logs apply to flow logs. Logs have a retention policy that can be set from 1 day to 365 days. If a retention policy is not set, the logs are maintained forever.

Diagnostic Logs

Periodic and spontaneous events are created by network resources and logged in storage accounts, sent to an Event Hub, or Log Analytics. These logs provide insights into the health of a resource. These logs can be viewed in tools such as Power BI and Log Analytics.

Diagnostic logs are available for Load Balancer, Network Security Groups, Routes, and Application Gateway.

Network Watcher provides a diagnostic logs view. This view contains all networking resources that support diagnostic logging. From this view, customers can enable and disable networking resources conveniently and quickly.

In addition to preceding logging capabilities, Network Watcher currently has the following capabilities:

- Topology: Provides a network level view showing the various interconnections and associations between network resources in a resource group.

- Variable Packet capture: Captures packet data in and out of a virtual machine. Advanced filtering options and fine-tuned controls such as being able to set time and size limitations provide versatility. The packet data can be stored in a blob store or on the local disk in .cap format.
- IP flow verifies: Checks if a packet is allowed or denied based on flow information 5-tuple packet parameters (Destination IP, Source IP, Destination Port, Source Port, and Protocol). If the packet is denied by a security group, the rule and group that denied the packet is returned.
- Next hop: Determines the next hop for packets being routed in the Azure Network Fabric, enabling customers to diagnose any misconfigured user-defined routes.
- Security group view: Gets the effective and applied security rules that are applied on a VM.
- Virtual Network Gateway and Connection troubleshooting: Provides the ability to troubleshoot Virtual Network Gateways and Connections.
- Network subscription limits: Enables customers to view network resource usage against limits.

Presidio Managed Services

Presidio Managed Services maintains an Audit Policy that defines how information is logged and audited. That policy also describes how it relates to each individual, how it is implemented, and how it is reported. The policy comprises of several key items.

Auditable Events

Presidio Managed Services' information system may generate audit records based on the following subjects: User authentication, System access, System Configuration Change, Audit Circumvention, System initialization, Program installation, Account modification, and/or the transfer of information out of the system. These events are necessary to support after-the-fact investigations of security incidents and will be periodically reviewed and updated.

Content of Audit Records

Presidio Managed Services' information system will produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Audit record content will include:

1. Date and time of the event
2. Component where the event occurred
3. Type of event
4. User/subject identity
5. Outcome (success or failure) of the event

Audit Storage Capacity

Sufficient audit record storage capacity will be allocated and configured to reduce the likelihood of such capacity being exceeded. The storage capacity will take into account the auditing to be performed, compliance requirements and the online audit processing requirements.

Audit Monitoring, Analysis, and Reporting

Presidio Managed Services regularly reviews information system audit records for indications of inappropriate or unusual activity, to investigate suspicious activity or suspected violations, may report findings to appropriate officials, and to take necessary actions. Presidio Managed Services employs automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications such as Gambling, Sexually-related, unapproved software downloads, copyright infringement, etc.

Time Stamps

Presidio Managed Services' systems will provide time stamps for use in audit record generation. Time stamps (including date and time) of audit records will be generated using internal system clocks and synchronizes with the internal information system clocks every ten minutes.

Protection of Audit Information

Audit information and audit tools will be protected from unauthorized access, modification, and deletion through authentication, cryptography and storage, as required. Audit information will include all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information systems activity.

Continuous Monitoring

Security controls monitoring in the system occurs on an ongoing basis. Presidio Managed Services will continuously monitor activities such as: configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. Continuous monitoring of security incidents and events is provided by the Security Incident and Event Management (SIEM) suite managed by the Security Operations Center.

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

Response:

AWS

AWS Identity and Access Management (IAM) enables customers to control access to AWS services and resources for their users securely. Using IAM, customers can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM allows customers to:

- **Manage IAM users and their access**: Customers can create users in IAM, assign them individual security credentials (i.e., access keys, passwords, and multi-factor

authentication devices) or request temporary security credentials to provide users access to AWS services and resources. Customers can manage permissions in order to control which operations a user can perform.

- **Manage IAM roles and their permissions**: Customers can create roles in IAM, and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. Customers can also define which entity is allowed to assume the role.
- **Manage federated users and their permissions**: Customers can enable identity federation to allow existing identities (e.g., users) in the enterprise to access the AWS Management Console, to call AWS APIs, and to access resources, without the need to create an IAM user for each identity.

Azure

Azure Role-Based Access Control (RBAC) helps customers to share various components available within an Azure subscription by providing fine-grained access management for Azure. Azure RBAC enables customers to segregate duties within their organization and grant access based on what users need to perform their jobs. Instead of giving everybody unrestricted permissions in Azure subscription or resources, customers can allow only certain actions.

Azure RBAC has three basic roles that apply to all resource types:

- Owner has full access to all resources including the right to delegate access to others.
- Contributor can create and manage all types of Azure resources but can't grant access to others.
- Reader can view existing Azure resources.

The rest of the RBAC roles in Azure allow management of specific Azure resources. For example, the Virtual Machine Contributor role allows the user to create and manage virtual machines. It does not give them access to the Azure Virtual Network or the subnet that the virtual machine connects to.

RBAC built-in roles list the roles available in Azure. It specifies the operations and scope that each built-in role grants to users.

Other capabilities for Azure Active Directory include:

- Azure AD enables SSO to SaaS applications, regardless of where they are hosted. Some applications are federated with Azure AD, and others use password SSO. Federated applications can also support user provisioning and password vaulting.
- Access to data in Azure Storage is controlled via authentication. Each storage account has a primary key (storage account key, or SAK) and a secondary secret key (the shared access signature, or SAS).
- Azure AD provides Identity as a Service through federation by using Active Directory Federation Services, synchronization, and replication with on-premises directories.

- Azure Multi-Factor Authentication is the multi-factor authentication service that requires users to verify sign-ins by using a mobile app, phone call, or text message. It can be used with Azure AD to help secure on-premises resources with the Azure Multi-Factor Authentication server, and also with custom applications and directories using the SDK.
- Azure AD Domain Services lets customers join Azure virtual machines to an Active Directory domain without deploying domain controllers. Customers can sign in to these virtual machines with their corporate Active Directory credentials and administer domain-joined virtual machines by using Group Policy to enforce security baselines on all their Azure virtual machines.
- Azure Active Directory B2C provides a highly available global-identity management service for consumer-facing applications that scales to hundreds of millions of identities. It can be integrated across mobile and web platforms. Customers' consumers can sign in to all their applications through customizable experiences by using their existing social accounts or by creating credentials.

Presidio Managed Services

Presidio Managed Services access control policy restricts visibility of documents to specific users and groups. Those access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by Presidio Managed Services to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. Access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for Presidio Managed Services.

Systems that are used for privileged functions and security-relevant information are restricted to authorized personnel, including security administrators, system and network administrators, and other privileged users. Privileged users include individuals who have access to system control, monitoring, or administration functions, including system administrators, information system security officers, maintainers, and system programmers.

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.

Response:

AWS

AWS has implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the AWS customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the AWS customer support team to alert customers to

any issues that may be of broad impact. The AWS Service Health Dashboard is accessible via the following link: http://status.aws.amazon.com/.

Azure

Please refer to our previous response to #8.3.1 in this section. Additional information regarding alerting customization capabilities is accessible via the following link: https://azure.microsoft.com/en-us/features/service-health/.

Presidio Managed Services

Monitoring occurs on a 24x7 basis and reasonable efforts are made to identify attacks promptly and reliably. In the event of a security incident, the methodology applied by the Intelligent Security Command Center (ISCC) analysts includes the following phases:

1. Preparation: Get ready to handle the security incident.
2. Identification: Detect the security incident.
3. Containment: Limit the impact of the security incident.
4. Remediation: Remove the threat.
5. Recovery: Recover to a normal posture.
6. Aftermath: Document and improve the process.

Please refer to our response to #8.6.13 in this section for additional information regarding these phases.

General actions to take for each step is determined on the type of security incident that has indications of occurring in the near future, is occurring currently, or has occurred.

The timing of the notifications and establishment of incident levels requires an impact and urgency assessment of the incident.

Impact refers to the business impact of the system impacted. The initial impact is pre-defined from the alerting tool, based on the type of alarm received or client request.

There are three categories of impact:

1. **High:** Incident affecting an entire site or multiple sites.
2. **Medium:** Incident affecting multiple users.
3. **Low:** Incident affecting one or few users.

Urgency is the extent to which the incident's resolution can bear delay. The initial urgency is pre-defined from the alerting tool, based on the type of alarm received or client request.

Presidio Incident and Problem urgency and corresponding priority levels are defined as follows:

1. **High:** Full service outage of a critical system or VIP is affected, requires urgent response.
2. **Medium:** Client's ability to function is partially impacted, requires the SDC to respond as soon as possible.
3. **Low:** No impact on the client's ability to function; is more informational in nature and a response is not critical.

Presidio retains the case priority even if there is a reduced severity of impact until incident resolution. The case may be left open for a prescribed period while operational stability is being assessed. Exhibit 6-6 outlines the incident priority assignment base on impact and urgency.

Exhibit 6-6. Incident Priorities

URGENCY	IMPACT: High	IMPACT: Medium	IMPACT: Low
High	P1	P2	P3
Medium	P2	P3	P4
Low	P3	P4	P4

Service Level Objectives (SLO) are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number and complexity and business impact of systems affected. Clients have the ability to set or change the priority level of an incident at any time, based on the impact to their specific business. Exhibit 6-7 describes the priority levels assigned. Exhibit 6-8 describes the Service Level Parameters.

Exhibit 6-7. Priority Levels

Level	Description
● **P1 / Critical**	Systems at one or many Client sites are completely unavailable. Affected systems cause significant business impact.
● **P2 / High**	Systems at one or many Client sites are partially unavailable. Affected systems cause some business impact.
● **P3 / Medium**	Operational performance of Client sites is impaired while most business operations remain functional.
● **P4 / Low**	Client is requesting information or a logical change that is covered under their service agreement.

Exhibit 6-8. Service Level Parameters

	Service Level Parameter	Agreement	Service Level
●	**P1 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	15 minutes	>95%
●	**P1 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	30 minutes	>95%
●	**P2 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	30 minutes	>90%
●	**P2 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	1 hour	>90%
●	**P3 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	4 hours	>80%
●	**P3 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	8 hours	>80%
●	**P4 Incidents - Remote Response Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	8 hours	NA
●	**P4 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	3 days	NA
●	**P4 Remote User Request Completion Time** Time to complete User request	8 business hours	NA

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.

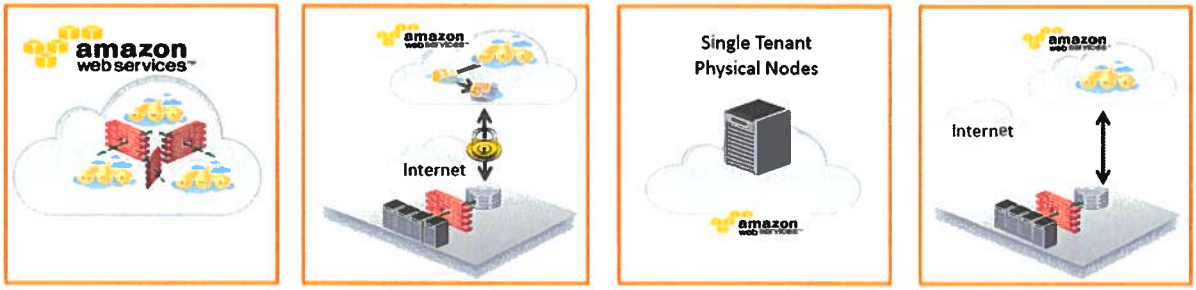
Response:

AWS

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization

software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016. More information on AWS's multi-tenant architecture is found in the "*AWS Risk and Compliance*" whitepaper accessible via the following link: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.

AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within the Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let customers take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating Amazon EC2 compute instances at the hardware level. AWS isolation and deployment options are illustrated in Exhibit 6-9.



Network Security Groups	Amazon Virtual Private Cloud (VPC)	Dedicated Instances	AWS Direct Connect
Flexible, named network access policy objects attached to VMs, dynamically updateable, enforced by the hypervisor	Create logically isolated AWS subnets in the AWS cloud and connect them with your corporate datacenter via a secure VPN connection	Run your virtualized operating systems and apps in a "single tenant per physical node" model within the AWS infrastructure	Dedicated, private, fast Layer 2 connectivity between your datacenter and the AWS cloud; no traffic on the Internet (available in some regions)

Exhibit 6-9. AWS Isolation and Deployment Options

Azure

Compute Isolation

Microsoft Azure provides various cloud-based computing services that include a wide selection of compute instances and services that can scale up and down automatically to meet the needs of a customer's application or enterprise. These compute instance and service offer isolation at multiple levels to secure data without sacrificing the flexibility in configuration that customers demand.

Isolated Virtual Machine Sizes

Azure Compute offers virtual machine sizes that are Isolated to a specific hardware type and dedicated to a single customer. These virtual machine sizes are best suited for workloads that require a high degree of isolation from other customers for workloads involving elements like compliance and regulatory requirements. Customers can also choose to further subdivide the resources of these isolated virtual machines by using Azure support for nested virtual machines.

Utilizing an isolated size guarantees that a customer's virtual machine will be the only one running on that specific server instance. The current isolated virtual machine offerings include:

- Standard_E64is_v3
- Standard_E64i_v3
- Standard_M128ms
- Standard_GS5
- Standard_G5
- Standard_DS15_v2
- Standard_D15_v2

Hyper-V and Root OS Isolation Between Root VM and Guest VMs

Azure's compute platform is based on machine virtualization—meaning that all customer code executes in a Hyper-V virtual machine. On each Azure node (or network endpoint), there is a Hypervisor that runs directly over the hardware and divides a node into a variable number of Guest Virtual Machines (VMs).

Each node also has one special Root VM, which runs the Host OS. A critical boundary is the isolation of the root VM from the guest VMs and the guest VMs from one another, managed by the hypervisor and the root OS. The hypervisor/root OS pairing leverages Microsoft's decades of operating system security experience, and more recent learning from Microsoft's Hyper-V, to provide strong isolation of guest VMs.

The Azure platform uses a virtualized environment. User instances operate as standalone virtual machines that do not have access to a physical host server, and this isolation is enforced by using physical processor (ring-0/ring-3) privilege levels.

Ring 0 is the most privileged and 3 is the least. The guest OS runs in a lesser-privileged Ring 1, and applications run in the least privileged Ring 3. This virtualization of physical resources leads to a clear separation between guest OS and hypervisor, resulting in additional security separation between the two.

The Azure hypervisor acts like a micro-kernel and passes all hardware access requests from guest virtual machines to the host for processing by using a shared-memory interface called VMBus. This prevents users from obtaining raw read/write/execute access to the system and mitigates the risk of sharing system resources.

Advanced VM placement Algorithm and Protection from Side Channel Attacks

Any cross-VM attack involves two steps: placing an adversary-controlled VM on the same host as one of the victim VMs, and then breaching the isolation boundary to either steal sensitive victim information or affect its performance for greed or vandalism. Microsoft Azure provides protection at both steps by using an advanced VM placement algorithm and protection from all known side channel attacks, including noisy neighbor VMs.

Azure Fabric Controller

The Azure Fabric Controller is responsible for allocating infrastructure resources to tenant workloads, and it manages unidirectional communications from the host to virtual machines. The VM placing algorithm of the Azure fabric controller is highly sophisticated and nearly impossible to predict as physical host level.

The Azure hypervisor enforces memory and process separation between virtual machines, and it securely routes network traffic to guest OS tenants. This eliminates possibility of and side channel attack at VM level.

In Azure, the root VM is special; it runs a hardened operating system called the root OS that hosts a fabric agent (FA). FAs are used in turn to manage guest agents (GA) within guest OSes on customer VMs. FAs also manage storage nodes.

The collection of Azure hypervisor, root OS/FA, and customer VMs/GAs comprises a compute node. FAs are managed by a fabric controller (FC), which exists outside of compute and storage nodes (compute and storage clusters are managed by separate FCs). If a customer updates their application's configuration file while it is running, the FC communicates with the FA, which then contacts GAs, which notifies the application of the configuration change. In the event of a hardware failure, the FC will automatically find available hardware and restart the VM there.

Communication from a Fabric Controller to an agent is unidirectional. The agent implements an SSL-protected service that only responds to requests from the controller. It cannot initiate connections to the controller or other privileged internal nodes. The FC treats all responses as if they were untrusted.

Isolation extends from the Root VM from Guest VMs, and the Guest VMs from one another. Compute nodes are also isolated from storage nodes for increased protection.

The hypervisor and the host OS provide network packet - filters to help assure untrusted virtual machines cannot generate spoofed traffic or receive traffic not addressed to them, direct traffic to protected infrastructure endpoints, or send/receive inappropriate broadcast traffic.

Additional Rules Configured by Fabric Controller Agent to Isolate VM

By default, all traffic is blocked when a virtual machine is created, and then the fabric controller agent configures the packet filter to add rules and exceptions to allow authorized traffic.

There are two categories of rules that are programmed:

- Machine configuration or infrastructure rules: By default, all communication is blocked. There are exceptions to allow a virtual machine to send and receive DHCP and DNS traffic. Virtual machines can also send traffic to the "public" internet and send traffic to other virtual machines within the same Azure Virtual Network and the OS activation server. The virtual machines' list of allowed outgoing destinations does not include Azure router subnets, Azure management, and other Microsoft properties.
- Role configuration file: This defines the inbound Access Control Lists (ACLs) based on the tenant's service model.

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).

Response:

AWS

The following AWS reference architectures support SaaS, IaaS, and PaaS:

- *"Architecting for the Cloud: AWS Best Practices"* contains prescriptive guidance for architects designing solutions with AWS services (https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf).
- *"Managing Your AWS Infrastructure at Scale"* contains information on tools and techniques for managing an AWS environment at any scale (https://d0.awsstatic.com/whitepapers/managing-your-aws-infrastructure-at-scale.pdf).
- *"AWS Well-Architected Framework"* addresses general design principles and provides specific best practices and guidance for architecture validation (https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)
- *"Amazon EC2 Reserved Instances and Other AWS Service Reservation Models"* provides IaaS and PaaS architecture fundamentals (https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-reservation-models/cost-optimization-reservation-models.pdf#introduction).
- *"An Overview of the AWS Cloud Adoption Framework"* provides recommendations for successful cloud adoption (https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf)

Additional reference materials are accessible online via the following link: https://aws.amazon.com/whitepapers/.

Azure

The Azure reference architectures, accessible via the following link support SaaS, IaaS, and PaaS: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/.

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.

Response:

AWS

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and customers are responsible for securing the workloads they deploy in AWS. AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts.

AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The AWS SOC report provides additional details regarding the controls in place for background verification.

Azure

Please refer to our previous response to #8.5.3 in this section.

Presidio Managed Services

As a pre-condition of employment, new hires must undergo a background check by a third-party vendor, regardless of position. Effort is made to verify all information provided by applicants on employment applications, including social security numbers and employment history. Other areas that are investigated include the applicant's criminal, educational, civil court, credit, and driving records. To investigate fully, the background check looks back 7 years at the following items:

- Social Security Number Trace/Death Master Search,
- County Criminal Court Records (Performed within the states that the candidate has lived, worked, and educated in),
- Federal Criminal Court Records,
- Multi State Sex Offender Registry,
- Government Sanctions Registry,
- Employment Verification,
- Education Verification (Highest Level Attained),
- 10 Panel Drug Screening,
- Department of Motor Vehicles (DMV), and
- Trans Union Credit Check.

Role Based Access Control is employed to limit access to only what the analyst requires to provide the contracted Managed Services. Active Directory, Dual Factor Authentication, VPN, SIEM monitoring, ITIL framework and our 24/7/365 Intelligent Security Command Center (ISCC) are utilized as technical security controls to protect client data should the administrative security controls not be sufficient.

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.

Response:

AWS

AWS customers retain control and ownership of their data, and all data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS offers the ability to add an additional layer of security to data at rest in the cloud by providing scalable and efficient encryption features. This includes:

- Data encryption capabilities in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Oracle RDS, SQL Server RDS, and Amazon Redshift.
- Flexible key management options, including AWS Key Management Service, that allow customers to choose whether to have AWS manage the encryption keys or keep complete control over their keys.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing customers to satisfy compliance requirements.
- Support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit.
- APIs for customers to integrate encryption and data protection with any of the services developed or deployed in an AWS environment.

The AWS Security Best Practices whitepaper provides greater detail on how to protect data in transit and at rest in the AWS Cloud. This whitepaper is accessible via the following link: https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf. Other security resources are also available on AWS's Cloud Security Resources page accessible via the following link: https://aws.amazon.com/security/security-resources/.

Azure

Encryption of Data at Rest

Data at rest includes information that resides in persistent storage on physical media, in any digital format. The media can include files on magnetic or optical media, archived data, and data backups. Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage. Microsoft also provides encryption to protect Azure SQL Database, Azure Cosmos DB, and Azure Data Lake. Data encryption at rest is available for services across the Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) cloud models.

Azure Encryption Models

Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. With client-side encryption, customers can manage and store keys on-premises or in another secure location.

Client-side Encryption

Client-side encryption is performed outside of Azure. It includes:

- Data encrypted by an application that is running in the customer's datacenter or by a service application.
- Data that is already encrypted when it is received by Azure.

With client-side encryption, cloud service providers do not have access to the encryption keys and cannot decrypt this data. Customers maintain complete control of the keys.

Server-side Encryption

The three server-side encryption models offer different key management characteristics, which customers can choose according to their requirements:

- Service-managed keys: Provides a combination of control and convenience with low overhead.
- Customer-managed keys: Gives customers control over the keys, including Bring Your Own Keys (BYOK) support, or allows customers to generate new ones.
- Service-managed keys in customer-controlled hardware: Enables customers to manage keys in a proprietary repository, outside of Microsoft control. This characteristic is called Host Your Own Key (HYOK). However, configuration is complex, and most Azure services do not support this model.

Azure Disk Encryption

Customers can protect Windows and Linux virtual machines by using Azure disk encryption, which uses Windows BitLocker technology and Linux DM-Crypt to protect both operating system disks and data disks with full volume encryption.

Encryption keys and secrets are safeguarded in the Azure Key Vault subscription. By using the Azure Backup service, customers can back up and restore encrypted virtual machines (VMs) that use Key Encryption Key (KEK) configuration.

Azure Storage Service Encryption

Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios.

Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when it is retrieved. The process is completely transparent to users. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES)

encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.

Client-side Encryption of Azure Blobs

Customers can perform client-side encryption of Azure blobs in various ways. Customers can use the Azure Storage Client Library for .NET NuGet package to encrypt data within client applications prior to uploading it to Azure storage.

When customers use client-side encryption with Key Vault, the data is encrypted using a one-time symmetric Content Encryption Key (CEK) that is generated by the Azure Storage client SDK. The CEK is encrypted using a Key Encryption Key (KEK), which can be either a symmetric key or an asymmetric key pair. Customers can manage it locally or store it in Key Vault. The encrypted data is then uploaded to Azure Storage.

Finally, customers can also use the Azure Storage Client Library for Java to perform client-side encryption before uploading data to Azure Storage, and to decrypt the data when downloading it to the client. This library also supports integration with Key Vault for storage account key management.

Encryption of Data at Rest with Azure SQL Database

Azure SQL Database is a general-purpose relational database service in Azure that supports structures such as relational data, JSON, spatial, and XML. SQL Database supports both server-side encryption via the Transparent Data Encryption (TDE) feature and client-side encryption via the Always Encrypted feature.

Transparent Data Encryption (TDE)

TDE is used to encrypt SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files in real time, using a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery.

TDE protects data and log files, using AES and Triple Data Encryption Standard (3DES) encryption algorithms. Encryption of the database file is performed at the page level. The pages in an encrypted database are encrypted before they are written to disk and are decrypted when they're read into memory. TDE is now enabled by default on newly created Azure SQL databases.

Always Encrypted Feature

With the Always Encrypted feature in Azure SQL, customers can encrypt data within client applications prior to storing it in Azure SQL Database. Customers can also enable delegation of on-premises database administration to third parties and maintain separation between those who own and can view the data, and those who manage it but should not have access to it.

Cell-level or Column-level Encryption

With Azure SQL Database, customers can apply symmetric encryption to a column of data by using Transact-SQL. This approach is called cell-level encryption or column-level encryption (CLE), because customers can use it to encrypt specific columns or even specific cells of data

with different encryption keys. Doing so gives customers more granular encryption capability than TDE, which encrypts data in pages. CLE has built-in functions that customers can use to encrypt data by using either symmetric or asymmetric keys, the public key of a certificate, or a passphrase using 3DES.

Cosmos DB Database Encryption

Azure Cosmos DB is Microsoft's globally distributed, multi-model database. User data that is stored in Cosmos DB in non-volatile storage (solid-state drives) is encrypted by default. There are no controls to turn it on or off. Encryption at rest is implemented by using a number of security technologies, including secure key storage systems, encrypted networks, and cryptographic APIs. Encryption keys are managed by Microsoft and are rotated per Microsoft internal guidelines.

At-rest Encryption in Data Lake

Azure Data Lake is an enterprise-wide repository of every type of data collected in a single place prior to any formal definition of requirements or schema. Data Lake Store supports "on by default," transparent encryption of data at rest, which is set up during the creation of the account. By default, Azure Data Lake Store manages the keys for customers, but customers have the option to manage them. Three types of keys are used in encrypting and decrypting data: the Master Encryption Key (MEK), Data Encryption Key (DEK), and Block Encryption Key (BEK). The MEK is used to encrypt the DEK, which is stored on persistent media, and the BEK is derived from the DEK and the data block. If customers are managing their own keys, they can rotate the MEK. Encryption of data in transit Azure offers many mechanisms for keeping data private as it moves from one location to another.

TLS/SSL Encryption in Azure

Microsoft uses the Transport Layer Security (TLS) protocol to protect data when it is traveling between the cloud services and customers. Microsoft data centers negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

Azure Storage Transactions

When customers interact with Azure Storage through the Azure portal, all transactions take place over HTTPS. Customers can also use the Storage REST API over HTTPS to interact with Azure Storage. Customers can enforce the use of HTTPS when they call the REST APIs to access objects in storage accounts by enabling the secure transfer that is required for the storage account.

Shared Access Signatures (SAS), which can be used to delegate access to Azure Storage objects, include an option to specify that only the HTTPS protocol can be used when customers use

Shared Access Signatures. This approach ensures that anybody who sends links with SAS tokens uses the proper protocol.

SMB 3.0, which used to access Azure Files shares, supports encryption, and it is available in Windows Server 2012 R2, Windows 8, Windows 8.1, and Windows 10. It allows cross-region access and even access on the desktop.

Client-side encryption encrypts the data before it is sent to the customer's Azure Storage instance, so that it is encrypted as it travels across the network.

SMB Encryption over Azure Virtual Networks

By using SMB 3.0 in VMs that are running Windows Server 2012 or later, customers can make data transfers secure by encrypting data in transit over Azure Virtual Networks. By encrypting data, customers help protect against tampering and eavesdropping attacks. Administrators can enable SMB encryption for the entire server, or just specific shares. By default, after SMB encryption is turned on for a share or server, only SMB 3.0 clients are allowed to access the encrypted shares.

In-transit Encryption in VMs

Data in transit to, from, and between VMs that are running Windows is encrypted in a number of ways, depending on the nature of the connection.

RDP Sessions

Customers can connect and sign in to a VM by using the Remote Desktop Protocol (RDP) from a Windows client computer, or from a Mac with an RDP client installed. Data in transit over the network in RDP sessions can be protected by TLS. Customers can also use Remote Desktop to connect to a Linux VM in Azure.

Secure access to Linux VMs with SSH

For remote management, customers can use Secure Shell (SSH) to connect to Linux VMs running in Azure. SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. It is the default connection protocol for Linux VMs hosted in Azure. By using SSH keys for authentication, customers eliminate the need for passwords to sign in. SSH uses a public/private key pair (asymmetric encryption) for authentication.

Azure VPN Encryption

Customers can connect to Azure through a virtual private network that creates a secure tunnel to protect the privacy of the data being sent across the network.

Azure VPN gateways

Customers can use an Azure VPN gateway to send encrypted traffic between their virtual network and their on-premises location across a public connection, or to send traffic between virtual networks. Site-to-site VPNs use IPsec for transport encryption. Azure VPN gateways use a set of default proposals. Customers can configure Azure VPN gateways to use a custom IPsec/IKE policy with specific cryptographic algorithms and key strengths, rather than the Azure default policy sets.

Point-to-site VPNs

Point-to-site VPNs allow individual client computers access to an Azure virtual network. The Secure Socket Tunneling Protocol (SSTP) is used to create the VPN tunnel. It can traverse firewalls (the tunnel appears as an HTTPS connection). Customers can use their own internal public key infrastructure (PKI) root certificate authority (CA) for point-to-site connectivity. Customers can configure a point-to-site VPN connection to a virtual network by using the Azure portal with certificate authentication or PowerShell.

Site-to-site VPNs

Customers can use a site-to-site VPN gateway connection to connect their on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires an on-premises VPN device that has an external-facing public IP address assigned to it. Customers can configure a site-to-site VPN connection to a virtual network by using the Azure portal, PowerShell, or Azure CLI.

In-transit Encryption in Data Lake

Data in transit (also known as data in motion) is also always encrypted in Data Lake Store. In addition to encrypting data prior to storing it in persistent media, the data is also always secured in transit by using HTTPS. HTTPS is the only protocol that is supported for the Data Lake Store REST interfaces.

Key Management with Key Vault

Without proper protection and management of the keys, encryption is rendered useless. Key Vault is the Microsoft-recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions to access keys can be assigned to services or to users through Azure Active Directory accounts. Key Vault relieves organizations of the need to configure, patch, and maintain hardware security modules (HSMs) and key management software. When customers use Key Vault, they maintain control. Microsoft never sees customers' keys, and applications do not have direct access to them. Customers can also import or generate keys in HSMs.

Presidio Managed Services

Presidio Managed Services maintains an access enforcement policy to secure the confidentiality of data at rest. Our access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by Presidio Managed Services to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. Access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for Presidio Managed Services.

Systems that are used for privileged functions and security-relevant information are restricted to authorized personnel, including security administrators, system and network administrators, and other privileged users. Privileged users include individuals who have access to system control,

monitoring, or administration functions, including system administrators, information system security officers, maintainers, and system programmers.

Presidio Managed Services leverages information flow enforcement to secure the confidentiality of data in transit. We ensure all information systems enforce approved authorizations for controlling the flow of information with the system and between interconnected systems based on defined flow control diagrams. Information flow controls where information is allowed to travel within an information system and between information systems and without explicit regard to subsequent accesses to that information.

Controlled information will be kept from being transmitted in the clear to the Internet through VPN usage, block outside traffic that claims to be from within Presidio Managed Services via our firewalls, and not pass any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms will control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems utilizing an interconnected routing system.

Flow control enforcement is based on the characteristics of the information and/or the information path. Boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) will employ rule sets and configuration settings that restrict information system services to provide a packet filtering capability.

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.

Response:

AWS

AWS services are content agnostic in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which customers store content. Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to place in the AWS cloud, only the customer can determine what level of security is appropriate for content stored and processed using AWS. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches, and to notify regulators and affected individuals as required under applicable law.

AWS has implemented a formal, documented incident response policy and program. Developed in alignment with the ISO 27001 standard, this policy addresses purpose, scope, roles, responsibilities, and management commitment, and ensures system utilities are appropriately restricted and monitored. An outline of AWS's three-phased approach to managing incidents follows:

2) **Activation and Notification Phase**: Incidents for AWS begin with the detection of an event. This can come from several sources including:
   a) Metrics and alarms: AWS maintains an exceptional situational awareness capability; most issues are rapidly detected from 24x7x365 monitoring and alarming of real-time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
   b) Trouble ticket entered by an AWS employee.
   c) Calls to the 24X7X365 technical support hotline: If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g., Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.
4) **Recovery Phase:** The relevant resolvers will perform break fix to address the incident. After troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and actions, and end the call engagement.
5) **Reconstitution Phase:** After the relevant fix activities are complete, the call leader will declare that the recovery phase is complete. Post mortem and deep-root-cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions, such as design changes etc., will be captured in a Correction of Errors (COE) document and tracked to completion.

In addition to internal communication mechanisms, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

The AWS incident management program is reviewed by independent external auditors during audits for SOC, PCI DSS, ISO 27001, and FedRAMP compliance. Additionally, the AWS incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Plans are tested and updated through the due course of business (at least monthly).

Azure

Detection of Potential Breaches

Due to the nature of modern cloud computing, not all data breaches occurring in a customer cloud environment involve Microsoft Azure services. Microsoft employs a shared responsibility model for Azure services to define security and operational accountabilities. Shared responsibility is particularly important when discussing security of a cloud service, because both the cloud services provider and the customer are accountable for portions of cloud security.

Microsoft does not monitor for or respond to security incidents within the customer's realm of responsibility. A customer-only security compromise would not be processed as an Azure security incident and would require the customer tenant to manage the response effort. Customer incident response may involve collaboration with Microsoft Azure customer support, given appropriate service contracts. Microsoft Azure also offers various services (e.g., Azure Security Center) that customers can utilize for developing and managing security incident response.

Azure responds to a potential data breach according to the security incident response process, which is a subset of the Microsoft Azure incident management plan. Azure's security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An overview of the security incident response process follows:

1. **Detect**: First indication of a potential incident.
2. **Assess**: An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.
3. **Diagnose**: Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, execution of the Customer Incident Notification process begins in parallel.
4. **Stabilize and Recover**: The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
5. **Close and Post-Mortem**: The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.

The detection processes used by Microsoft Azure are designed to discover events that risk the confidentiality, integrity, and availability of Azure services. Several events can trigger an investigation:

- Automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection, or via algorithms designed to profile expected activity and alert upon anomalies.
- First-party reports from Microsoft Services running on Microsoft Azure and Azure Government.
- Security vulnerabilities are reported to the Microsoft Security Response Center (MSRC) via secure@microsoft.com. MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.

- Customer reports via the Customer Support Portal, or Microsoft Azure and Azure Government Management Portal, that describe suspicious activity attributed to the Azure infrastructure (as opposed to activity occurring within the customer's scope of responsibility).
- Security Red Team and Blue Team activity. This strategy uses a highly-skilled Red Team of offensive Microsoft security experts to uncover and attack potential weaknesses in Azure. The security response Blue Team must detect and defend against the Red Team's activity. Both Red and Blue Team actions are used to verify that Azure security response efforts are effectively managing security incidents. Security Red Team and Blue Team activities are operated under rules of engagement to help ensure the protection of customer data.
- Escalations by operators of Azure Services. Microsoft employees are trained to identify and escalate potential security issues.

Azure's Data Breach Response

Microsoft assigns the investigation appropriate priority and severity levels by determining the functional impact, recoverability, and information impact of the incident. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked around the clock to resolution. Microsoft Azure categorizes the information impact of the incident into the following breach categories:

- None: No information was exfiltrated, changed, deleted, or otherwise compromised.
- Privacy Breach: Sensitive personal data of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated.
- Proprietary Breach: Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated.
- Integrity Loss: Sensitive or proprietary information was changed or deleted.

The Security Response Team works with Microsoft Azure Security Engineers and SMEs to classify the event based on factual data from the evidence. A security event may be classified as:

- False Positive: An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team will identify the root cause for false positives and will address them in a systematic way leveraging detection sources and fine-tuning them as needed.
- Security Incident: An incident where unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data has occurred.

- Customer-Reportable Security Incident (CRSI): An unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of customer data.
- Privacy Breach: A subtype of Security Incident involving personal data. Handling procedures are no different than a security incident.

For a CRSI to be declared, Microsoft must determine that unauthorized access to customer data has or has very likely occurred, and/or that there is a legal or contractual commitment that notification must occur. It is desired, but not required, that specific customer impact, resource access, and repair steps be known. An incident is generally declared a CRSI after the conclusion of the Diagnose stage of a security incident; however, the declaration may happen at any point that all pertinent information is available. The security incident manager must establish evidence beyond reasonable doubt that a reportable event has occurred to begin execution of the Customer Incident Notification Process.

Throughout the investigation, the security response team works closely with global legal advisors to help ensure forensics are performed in accordance with legal obligations and commitments to customers. There are also significant restrictions on system and customer data viewing and handling in various operating environments. Sensitive or confidential data, as well as Customer Data, are not transferred out of the production environment without explicit written approval from the Incident Manager recorded in the corresponding incident ticket.

Microsoft verifies that customer and business risk is successfully contained, and that corrective measures are implemented. If necessary, emergency mitigation steps to resolve immediate security risks associated with the event are taken.

Microsoft also completes an internal post-mortem for data breaches. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the Security Incident Response SOP or related processes are identified and implemented. Internal post-mortems for data breaches are highly confidential records not available to customers. Post-mortems may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of Azure's routine audit cycle.

Customer Notification

Microsoft Azure notifies customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of Azure. Data flow logs are also robust. As a benefit of this design, most incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

After the declaration of a CRSI, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered in no more than 72 hours from the time Microsoft declared a breach except for the following circumstances:

- Microsoft believes the act of performing a notification will increase the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- Other unusual or extreme circumstances vetted by Microsoft's legal department Corporate External and Legal Affairs (CELA) and the Executive Incident Manager.

Microsoft Azure provides customers with detailed information enabling them to perform internal investigations and assisting them in meeting end user commitments, while not unduly delaying the notification process.

Notification of a personal data breach will be delivered to the customer by any means Microsoft selects, including via email. Notification of a data breach will be delivered to the list of security contacts provided in Azure Security center. If contact information is not provided in Azure Security Center, the notification will be sent to one or more administrator in an Azure subscription. To ensure notification can be successfully delivered, it is the customer's responsibility to ensure the administrative contact information on each applicable subscription and online services portal is correct.

The Microsoft Azure or Azure Government team may also elect to notify additional Microsoft personnel such as Customer Service (CSS) and the customer's Account Manager(s) (AM), or Technical Account Manager(s) (TAM). These individuals often have close relationships with the customer and can facilitate faster remediation.

Presidio Managed Services

The Presidio Managed Services incident response plan is based on industry-standard incident response framework consisting of these seven phases:

1. Preparation
    a. Formation of Computer Incident Response Team
    b. Incident response training of CIRT members
    c. Technical incident handling training for IT and security staff
    d. Contact list for CIRT members, law enforcement, payment card brands and acquiring bank
    e. Annual incident response testing
2. Detection
    a. Observation of anomalous event
3. Analysis
    a. Determine scope of incident
    b. Assign severity to incident
4. Containment
    a. System isolation

b. Forensically sound system backups

5. Eradication
   a. Removing unauthorized code
   b. Applying patches
   c. Installing Security Software
   d. Removing unnecessary services
6. Recovery
   a. Rebuilding of systems
   b. Operating system and application hardening
   c. Clean backup restoration
7. Post-Incident Activity/Lessons Learned
   a. Forensic review report
   b. Re-evaluation of security infrastructure

Card brands and acquiring banks must be notified upon discovery of a data security breach involving cardholder data. Visa and many acquiring banks may require a forensic review of a cardholder data security breach by a Qualified Incident Response Assessor (QIRA).

Preparation Phase

Computer Incident Response Team (CIRT) Requirements

The Computer Incident Response Team is comprised of employees from both management and Information Security with the required skills to identify and control system compromises or other intrusion incidents.

1. List the members and the roles and responsibilities of the Computer Incident Response Team. (Refer to Exhibit 6-10.)
2. Train the members of the Computer Incident Response Team to deal with security breach incidents.
3. Ensure availability of team members at all times (24/7) to respond to alerts, intrusion detection, or other incidents.
4. Train members of the Computer Incident Response Team to keep current with technical developments in the industry.
5. Notify the Computer Incident Response Team Leader of any unauthorized activity, critical IDS alerts, or reports of unauthorized critical system or content file changes and determine the need to activate the full Incident Response Plan.

Exhibit 6-10. Recommended CIRT Members

CIRT Members	CIRT Role
Senior Management	Provide authority to operate and has authority to make business-related decisions based on information garnered from the other team members.
Information Security	Assess security incidents, perform containment, eradication and basic forensics. Assist information technology in recovery role.
Information Technology	Minimize the impact to system end users. Assist the Information Security team with technical issues and recovery roles.
Audit	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.
Physical Security	Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.
Legal	Ensure evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.
Human Resources	Provide advice to senior management if an employee caused the incident.
Public Relations	Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands and law enforcement to develop a disclosure plan (if any).

Incident Response Plan – Annual Review and Testing

Regular review and testing of the Presidio Managed Services Incident Response Plan is essential to maintain compliance with the Payment Card Industry Data Security Standard.

The following must be completed at least annually to maintain compliance with the PCI Data Security Standard. Documentation of completion is required.

1. Review the Incident Response Plan annually and modify as necessary to ensure it is up to date according to lessons learned and industry developments.
2. Test the Incident Response Plan annually.

Detection and Analysis Phases

The Incident Response Plan includes continuous monitoring with the ability to send real time alerts to appropriate personnel from intrusion detection, intrusion prevention, and file integrity monitoring systems for all critical systems components.

A detailed process or procedure for monitoring critical security breach indicators (event logs, IDS logs, File Integrity report, wireless scans or wireless IDS logs, wireless access point ID, etc.) must be defined and documented in the IRP.

Presidio Managed Services monitors its cardholder environment utilizing LogRhythm SIEM solution and 24/7/365 Security Analysts for immediate analysis. This solution provides the initial and follow-up evidence for all security incidents that may present themselves in this environment.

Use the incident response form to help assigned personnel with the identification and initial assessment of security incidents. The form helps incident responders gather information necessary to confirm the existence of an incident. Information gathered allows CIRT members to determine the scope and potential impact of an incident. Any incident involving the compromise or suspected compromise of cardholder information must be reported to impacted card brands, the acquiring bank and any other entities as required by contract or law.

PMN Security Incident Escalation and Response Process is utilized to determine Presidio Managed Services specific Severity, Urgency, and Priority of the Security Incident to ensure the proper personnel that may not be included on the PMN Security Incident Response Contact list for initial response are notified in a timely manner to assist in the Incident Response Containment, Eradication, and Recovery.

Containment Phase

The containment phase allows Presidio Managed Services incident handlers to regain control of the situation and to minimize the amount of impact caused by an incident. Incident handlers must take careful steps to contain systems storing, transmitting or processing cardholder information. The following general guidelines should be followed to protect evidence and limit the exposure of cardholder information:

- Perform system backup (backups must be forensically sound to preserve the machine state).
- Remove system from network.
- Change administrative, application and system passwords.
- Create additional firewall restrictions.

Business impact must be evaluated before removing a system from a production environment.

Eradication and Recovery Phases

During the eradication and recovery phases of an incident, the root cause of an incident must be determined. Qualified personnel must perform eradication and recovery phase incident response reports. Forensic analysis of system memory, disk storage and logs must be analyzed to determine the cause of the incident. Administrative tools found on the compromised system should not be used in the event the perpetrator has modified system tools.

Re-installing the operating system and restoring a known clean system backup should perform recovery. The full Presidio Managed Services systems hardening procedure must be followed prior to placing the system back into production. Once the system is placed back into production, increased monitoring and testing should be performed to validate that the eradication has been successful and that the root cause of the compromise has not persisted.

Card Association members may require Presidio Managed Services to contract with a Qualified Incident Response Assessor. For a list of Visa Inc. QIRAs, go to http://www.visa.com/cisp, under If Compromised section. The file is labeled "Qualified Incident Response Assessor List." Forensic work performed by a QIRA needs to be coordinated with the card brands and the acquiring bank.

Post-Incident Recovery and Lessons Learned Phase

Incident response plan tests and live incidents provide valuable insight into the effectiveness of the incident response plan. At the end of the incident response process, there is often a tendency to return to "business as usual" without updating Presidio Managed Services policies, procedures and guidelines. A post-mortem examination of the incident should be conducted to validate that Presidio Managed Services policies, procedures and guidelines are up to date and being followed. Any changes need to be documented and communicated to relevant personnel.

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.

Response:

AWS

AWS Customers manage the creation and deletion of their data on AWS, as well as maintain control of access permissions. Customers are responsible for maintaining appropriate data retention policies and procedures. Controls in place limit access to systems and data, and ensure access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits. Refer to the AWS SOC 1 audit report (available under AWS NDA) for more information and validation of the control testing related to access permissions and data deletion for AWS S3 Services. Refer to the AWS PCI Compliance Package (available under AWS NDA) for testing performed to confirm data deletion. Both the AWS SOC 1 audit report and the AWS PCI Compliance Package can be requested at http://aws.amazon.com/compliance/contact/.

Azure

Please refer to our previous response to #8.5.3 in this section. Additional information is accessible via the following link: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be394.

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.

Response:

AWS and Azure

AWS and Azure public cloud customers retain full ownership of their data. Prior to any system consolidation, clients must be well versed with ingress and egress between the public cloud and on-premises. Hence, the data can be procured via the wire (over the network) or via data transfer solutions offered by AWS and Azure. It must be noted that the magnitude of data might not always make it cost effective to perform data transfers over the network due to bandwidth and cost constrains. As such, batch services such as AWS Snowball (https://aws.amazon.com/snowball/), AWS Snowmobile (https://aws.amazon.com/snowmobile/), and Azure Data Box (https://azure.microsoft.com/en-us/services/storage/databox/) are available for large data transfer solutions in the terabyte to petabyte range while offering high encryption standards.

8.8 (E) SERVICE OR DATA RECOVERY

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

b. Suffers an unrecoverable loss of data.

c. Offeror experiences a system failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Response:

AWS

The following AWS fundamental design patterns and platform capabilities apply to #8.8.1 and 8.8.2 requirements.

Availability and Fault-Tolerant Design

Amazon's infrastructure has a high level of availability and provides the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data

traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, the data centers are each powered via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

Each customer or Purchasing Entity should architect AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures. However, agencies or Purchasing Entities should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between regions unless proactively done so by the customer, thus allowing customers with these types of data placement and privacy requirements the ability to establish compliant environments. It should be noted that all communications between regions is across public Internet infrastructure; therefore, appropriate encryption methods should be used to protect sensitive data.

As of this writing, AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage.

AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move workloads into the cloud by helping them meet certain regulatory and compliance requirements. The AWS GovCloud (US) framework allows US government agencies and their contractors to comply with U.S. International Traffic in Arms Regulations (ITAR) regulations, as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. AWS GovCloud (US) has received an Agency Authorization to Operate (ATO) from the US Department of Health and Human Services (HHS) utilizing a FedRAMP accredited Third-Party Assessment Organization (3PAO) for several AWS services.

The AWS GovCloud (US) Region provides the same fault-tolerant design as other regions, with two Availability Zones. In addition, the AWS GovCloud (US) region is a mandatory AWS Virtual Private Cloud (VPC) service by default to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses.

Azure

Each service will adhere to the individual Microsoft SLAs for that service. Service status can be tracked via the following link: https://azure.microsoft.com/en-us/status/.

Presidio Managed Services

Extended Downtime and Unrecoverable Loss of Data

Presidio Managed Services follows an ITIL-based incident management process when addressing and resolving incidents in a customer environment. Presidio will perform the following during the management of incidents identified through monitoring of the environment or by direct Client notification:

- Event identification, logging and management
- Alert Review to assess if it is an actual alert or system anomaly
- Clear system anomalies and close the incident
- Group related relevant events into a single incident to reduce notifications
- Prioritize incidents based on impact and urgency
- Notify Client of the incident, according to the notification matrix, and within the notification service level
- Restore Service
    - Take complete ownership of service restoration or remotely assist onsite personnel as needed to facilitate service restoration.
    - Remotely facilitate hardware replacement and software updates determined to be required by Presidio.
    - Remotely apply patches to remediate an incident or problem identified by Presidio and handled as a Standard Change, if required.
    - Escalate to third-party support providers (e.g., AWS Business Support, Microsoft Azure Support) in the event of extended downtime related to availability of cloud services.

Data Recovery and Restoration After Severe System Outages

Presidio backup and recovery management offering provides comprehensive Managed Services for operating your data protection systems. The service encompasses the underlying backup software and appliances (hardware and software) as well as any hypervisors, operating systems, or applications that interact with the backup systems.

Presidio continuously monitors the environment to identify fault and performance conditions within the backup and recovery infrastructure, follows an incident management process to ensure conditions are properly cleared, and engages the customer throughout the incident life cycle. Presidio can also interface with the equipment vendor on the customer's behalf to remediate

conditions due to hardware failure, be engaged in the RMA process, and assist during the recovery process following replacement.

Presidio can also assist with and/or perform backup and recovery of data. Data backup and recovery requests can be submitted via email, web portal, or phone call to Presidio's service desk which is continuously available (24x7x365).

Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Presidio continuously monitors the environment to identify fault and performance conditions within the backup and recovery infrastructure, follows an incident management process to ensure conditions are properly cleared, and engages the customer throughout the incident life cycle. Presidio can also interface with the equipment vendor on the customer's behalf to remediate conditions due to hardware failure, be engaged in the RMA process, and assist during the recovery process following replacement. These aspects of our managed services ensure the backup and recovery infrastructure is functioning optimally so that if those services are needed designed RTO/RPO are achieved.

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.

Response:

AWS

Please refer to our preceding response to #8.8.1 in this section.

Azure

Azure utilizes storage replication for the majority of services, if elected by the customer, unless identified separately in the SLA. For additional information, refer to the SLA documents for each individual service. Data backup and retention is the responsibility of the customer. Azure utilizes a paired region approach to business continuity and disaster recovery. Additional information regarding Azure paired regions is accessible via the following link: https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions.

Presidio Managed Services

Data Backups

Our backup and recovery management offering provides comprehensive Managed Services for operating data protection systems. The service encompasses the underlying backup software and appliances (hardware and software), as well as any hypervisors, operating systems, or

applications that interact with the backup systems. Our services support our customers with a three-tier data backup model where we:

1. Create, maintain, and support backup job(s) and associated scheduling to meet customer backup objectives.
2. Support Snapshot and cloning activities at the virtual machine, file, and LUN level to enable a point in time recovery.
3. Implementation of data replication and associated scheduling between data replication devices within the customer's network to ensure off-site copies of data.

Server Image Backups

With our backup and recovery management offering, the operational aspects of server backup are critical components of our services, which extend beyond simply taking server backup images. Presidio will also:

- Implement minor software upgrades (i.e., dot releases) on all devices included as part of the covered equipment list. This ensures data protection systems are operating in an optimal state.
- Implement corrective actions to resolve failures associated with backup jobs to ensure backup data is available should the need arise.
- Create backup job(s) and associated scheduling to meet customer backup objectives.
- Implement snapshot and cloning activities at the virtual machine and LUN level to enable a point in time recovery.

Backup Storage Location

Our backup and recovery services have a specific service element supporting data replication to secondary devices for offsite data storage or backup to an onsite tape library. The service also includes minor software upgrades (i.e., dot releases) on all devices included as part of the covered equipment list, corrective actions to resolve failures associated with backup jobs, and activities to maintain data replication between data replication devices.

Alternate Data Center Strategies

Operationally, Presidio maintains three Service Delivery Centers from where services are delivered: Orlando, FL; Lewisville, TX; and Hauppauge, NY. Combined, these locations operate continuously (24x7x365) while providing both geographical and labor diversity. The locations leverage a common operations model that allows all locations to operate as a single, cohesive Service Delivery Center and enables other advantages, such as call distribution during high call volume conditions.

There are several technology platforms that Presidio leverages to deliver managed services to our customers. These on-premise applications are hosted in two, colocation data centers that are physically diverse. Each data center facility is compliant (e.g., SOC 2, SOC 3, PCI-DSS, etc.), located outside of a 500-year flood plain, and has generator backup capability, N+1 UPS redundancy, and N+1 cooling redundancy.

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.

Response:

AWS

Securing Data at Rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions (e.g., AWS Key Management Service [KMS]) to manual, client-side options (e.g., AWS CloudHSM). Choosing the right solutions depends on the AWS Cloud services being used and the customer requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide accessible online at the following link: https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html.

Additionally, the Encrypting Data at Rest whitepaper provides an overview of the options for encrypting data at rest in AWS Cloud services. It describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS Cloud services. The whitepaper is accessible online via the following link: https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf.

Azure

Please refer to our previous response to #8.6.12 in this section.

Presidio Managed Services

Presidio Managed Services also stores sensitive data (i.e., IP addresses, passwords, usernames, etc.) needed to deliver services. This information is classified as confidential according to our information classification policy; as such, we protect the data against unauthorized access and disclosure, modification, destruction, and use. Access to that information requires dual-factor authentication with each request being logged.

Securing Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

Services from AWS provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

Presidio Managed Services

Presidio Managed Services also secures all data in transit that is used to deliver services. We ensure all information systems enforce approved authorizations for controlling the flow of information with the system and between interconnected systems based on defined flow control diagrams. Information flow controls where information is allowed to travel within an information system and between information systems, and without explicit regard to subsequent accesses to that information.

Controlled information will be kept from being transmitted in the clear to the Internet through VPN usage, block outside traffic that claims to be from within Presidio Managed Services via our firewalls, and not pass any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms will control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems utilizing an interconnected routing system.

Flow control enforcement is based on the characteristics of the information and/or the information path. Boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) will employ rule sets and configuration settings that restrict information system services to provide a packet filtering capability.

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.

Response:

For Presidio, Trina Dennis-Carlson, Director – Contracts, will be responsible to sign any relevant and applicable Business Associate Agreement or any other agreement necessary to protect data with a Purchasing Entity.

AWS

AWS provides a standard Business Associate Addendum (BAA), which takes into account the unique services AWS offers and accommodates the AWS Shared Responsibility Model, to customers for signature.

Azure

Microsoft does not access or use customer content for any purpose other than as legally required and to provide the Azure services selected by each customer, to that customer and its end users. Azure never uses customer content or derives information from it for other purposes such as marketing or advertising.

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.

Response:

AWS

AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Azure

Please refer to our previous response to #8.5.3 in this section.

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.

Response:

AWS

AWS has millions of active customers and offers the same portfolio of self-service, highly automated web services to its customers on a one-to-many basis. Because of this, AWS does not typically negotiate SLAs for customers. AWS continually expands its services to support virtually any cloud workload, and it now has more than 100 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid, and enterprise applications.

Azure

While Microsoft SLAs are not negotiable, improved SLAs are available by utilizing highly available configurations as discussed in our response to #8.12.1 in this section.

Presidio Managed Services

The managed services delivered by Presidio include standard Service Level Objectives (SLO) that, through experience, we have found resonant with the majority of our customers. These SLOs are tightly integrated into our ITIL-based processes - incident management in particular, to

ensure customer satisfaction. These SLOs and any underlying processes can be modified to suit specific customer business requirements.

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.

Response:

Please refer to the sample SLAs provided in our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal.

Presidio Managed Services

Presidio's Managed Services have Service Level Objectives (SLO) that are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number, complexity, and business impact of systems affected. Clients have the ability to set or change the priority level of an incident at any time, based on the impact to their specific business. Exhibit 6-11 describes the priority levels assigned. Exhibit 6-12 describes the Service Level Parameters.

Exhibit 6-11. Priority Levels

Level	Description
● **P1 / Critical**	Systems at one or many Client sites are completely unavailable. Affected systems cause significant business impact.
● **P2 / High**	Systems at one or many Client sites are partially unavailable. Affected systems cause some business impact.
● **P3 / Medium**	Operational performance of Client sites is impaired while most business operations remain functional.
● **P4 / Low**	Client is requesting information or a logical change that is covered under their service agreement.

Exhibit 6-12. Service Level Parameters

	Service Level Parameter	Agreement	Service Level
●	**P1 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	15 minutes	>95%
●	**P1 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	30 minutes	>95%
●	**P2 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	30 minutes	>90%
●	**P2 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	1 hour	>90%
●	**P3 Incidents - Remote Response Acknowledge Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	4 hours	>80%
●	**P3 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	8 hours	>80%
●	**P4 Incidents - Remote Response Time** Total Problem Reports acknowledged within Service Level Target/Total Problem Reports	8 hours	NA
●	**P4 Incidents - Remote Access Response Time** Total Problem Reports within Remote Access Response Time Service Level Target/Total Problem Reports	3 days	NA
●	**P4 Remote User Request Completion Time** Time to complete User request	8 business hours	NA

Remote Response Acknowledge Time is the amount of elapsed time between Client initiations of an issue, or the time Presidio Managed Services detects a fault, and the time Presidio Managed Services creates an incident report and alerts Client that an incident has been created.

Remote Access Response Time is the amount of elapsed time between Client initiations of an issue, or the time Presidio Managed Services proactively detects a fault, and the time an assigned Presidio Managed Services technician connects to the system, or otherwise contacts Client, and begins remote diagnosis and troubleshooting.

Remote User Request Completion Time is the amount of elapsed time between Client request of a User Change and the completion of the change and measured in US business hours.

8.11 (E) DATA DISPOSAL

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

Response:

AWS

AWS provides customers with the ability to delete their data. AWS customers retain control and ownership of their data, and it is the customer's responsibility to manage their data.

AWS Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Azure

Microsoft is governed by strict standards and follows specific processes for removing cloud customer data from systems under its control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware.

Data Retention

In its Online Services Terms, Microsoft contractually commits to specific processes when a customer leaves a cloud service or the subscription expires. This includes deleting customer data from systems under its control.

If a customer terminates a cloud subscription or it expires (except for free trials), Microsoft will store customer data in a limited-function account for 90 days (the "retention period") to give the customer time to extract the data or renew the subscription. During this period, Microsoft provides multiple notices, so the customer will be amply forewarned of the upcoming deletion of data. After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period. (In-scope services are defined in the Data Processing Terms section of Microsoft Online Services Terms.) When customer data is hosted in the multitenant environments of Microsoft business cloud services, Microsoft takes careful measures to logically separate customer data. This helps prevent one customer's data from leaking into that of another customer, which also helps to block any customer from accessing another customer's deleted data.

Data Deletion on Physical Storage Devices

If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure the data cannot be recovered by any means. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

Presidio Managed Services

The Presidio Data Collection Appliance (DCA) is provided as part of Presidio's Managed Service offering. It provides a monitoring framework for Presidio to actively monitor the health and performance of managed configuration items included in the managed services agreement. At the end of the service agreement period, the DCA is returned to Presidio and all customer data is securely removed from the DCA using block level wiping software.

8.12 (E) PERFORMANCE MEASURES AND REPORTING

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Response:

AWS

How reliable is an application hosted by AWS?

In 2014, Nucleus Research surveyed 198 AWS customers that reported moving existing workloads from on-premises to AWS and found that they were able to reduce unplanned downtime by 32% (refer to Availability and Reliability in the Cloud: Amazon Web Services).

AWS takes extensive precautions to help ensure it will remain fully operational, with no loss of service for its hosted applications. AWS replicates critical system components across multiple Availability Zones to ensure high availability both under normal circumstances and during disasters such as fires, tornadoes, or floods. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS Availability Zone runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single Availability Zone. The data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations. Common points of failure, such as generators, UPS units, and air conditioning, are not shared across Availability Zones.

AWS plans for failure by maintaining contingency plans and regularly rehearsing its responses. In the words of Werner Vogels, Amazon's CTO: "Everything fails, all the time." AWS regularly performs preventative maintenance on generators and UPS units to ensure equipment is ready

when needed. AWS also maintains a series of incident response plans covering both common and uncommon events, and updates them regularly to incorporate lessons learned and prepare for emerging threats.

While AWS goes to great lengths to provide availability of its cloud platform, AWS customers share responsibility for ensuring availability within the cloud. These customers and others like them have succeeded because they designed for failure and have adopted best practices for high availability, such as taking advantage of multiple Availability Zones and configuring Auto Scaling groups to replace unhealthy instances. The Building Fault-Tolerant Applications on AWS whitepaper is a great introduction to achieving high availability in the cloud. In addition, the AWS Well-Architected Framework codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions.

In addition, the AWS Architecture Center is designed to provide customers with the necessary guidance and application architecture best practices to build highly scalable and reliable applications in the AWS Cloud. These resources help clients understand the AWS Cloud, its services and features, and provide architectural guidance for design and implementation of systems that run on the AWS infrastructure.

Azure

Service Level Agreements carry varying tiers based on high availability options chosen by the purchaser such as Availability Sets, Availability Zones, Fault Domains, Redundant VPN/ExpressRoute links, Geo-Redundant Storage, and other factors. Many resources offer a 99.99% uptime when configured using the highly available configurations offered by Microsoft Azure.

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

Response:

AWS

Please refer to our previous response to RFP section 5.3.4, which provides baseline SLA information, and is included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal." Additionally, AWS far exceeds the Uptime Institute Tiering certification (https://uptimeinstitute.com/TierCertification/). Tiering aspects do not take into consideration the nature of the services of the cloud environment, and although the Uptime Institution Tiering can be a great guide, it ultimately does not accurately map to a cloud service provider organization. AWS does not have a Certified Uptime Tiering level; however, AWS operates a data center environment using N+1 architecture. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95%, and Amazon S3 with an SLA of 99.9%. AWS's generator backup capabilities are detailed in AWS's System and Organization Control (SOC) Reports (https://aws.amazon.com/compliance/soc-faqs/) along with information concerning business continuity planning and N+1 architecture.

Azure

Please refer to our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal."

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.

Response:

AWS

AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced technical support engineers. The service helps customers of all sizes and technical abilities to successfully use the products and features provided by AWS.

AWS Support provides a highly personalized level of service for customers seeking technical help. Customers who do not choose AWS Support will continue to have access to Basic Support offered at no additional charge. All plans, including Basic Support, provide 24x7 access to customer service, AWS Documentation, Resource Center, Product FAQs, Discussion Forums, and support for Health Checks. All customers receive Basic Support included with an AWS account.

For access to technical support and additional AWS Support resources, AWS offers plans to fit a customer's unique needs. Exhibit 6-13 provides a comparison between AWS Basic, Developer, Business, and Enterprise support.

Exhibit 6-13. AWS Support Plans

	Basic	Developer	Business	Enterprise
Customer Service – 24x7x365	✓	✓	✓	✓
Support Forums	✓	✓	✓	✓
Documentation, Whitepapers, Best Practice Guides	✓	✓	✓	✓
Access to Technical Support	Support for Health Checks	Email (local business hours)	Phone, Chat, Email (24/7)	Phone, Chat, Email, Technical Account Manager (TAM) (24/7)
Primary Case Handling	Technical Customer Service Associate	Cloud Support Associate	Cloud Support Engineer	Sr. Cloud Support Engineer

	Basic	Developer	Business	Enterprise
Users Who Can Create Technical Support Cases		1	Unlimited (AWS Identity and Access Management [IAM] supported)	Unlimited (IAM supported)
Response Time		General guidance: < 24 business hours System impaired: < 12 business hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture Support		General Guidance	Contextual Use Case Guidance	Contextual Application Architecture Guidance
Access to Support API			✓	✓
Third-Party Software Support			✓	✓
AWS Trusted Advisor	4 core checks	4 core checks	Full checks	Full checks
Infrastructure Event Management				✓
Direct Access to TAM				✓
Architectural Review				✓
Support Concierge				✓
Training				Access to online self-paced labs
Operations Support				Operational reviews, recommendations, and reporting

All AWS Support tiers include an unlimited number of support cases, with no long-term contracts. Also, with the Business and Enterprise-level tiers, as customers' AWS charges grow, they earn volume discounts on AWS Support costs. For information on AWS Support pricing, visit the AWS Support Plan Pricing webpage accessible via the following link: https://aws.amazon.com/premiumsupport/pricing/.

Contacting AWS Support

Customers can contact AWS Support via AWS's online Support Center. All Developer-level support customers can open a case online with "Web Support" using a web browser. Business- and Enterprise-level customers may also "Click to Call" to have AWS contact them at any convenient phone number or strike up a conversation with an engineer via Chat. Enterprise-level customers also have a direct access to their dedicated TAM.

Chat is another way to contact AWS Support. By clicking on the chat support icon in the Support Center, a chat session will be initiated through the browser. This provides a real-time, one-on-one interaction with our support engineers and allows additional information and links to be shared for faster issue resolution.

Azure

Presidio is a Microsoft Solution Cloud Provider (CSP) partner and provides full, end-to-end, deployment to management support for our Microsoft customers. Our CSP support model is a 24x7 support offering that covers Level 1 and Level 2 support for Microsoft cloud offerings such as Azure. After a customer is onboarded as a Presidio Microsoft CSP customer and our solutions engineers assist with migration professional services, all support is managed through our well-established Managed Services organization. In addition to handling resolution of Level 1 and Level 2 support, our support offering works directly with Microsoft support experts to manage resolution of Level 3 support issues on the customer's behalf.

Making support easier for our customers is Presidio's goal. Presidio provides a toll-free phone number or access to an online self-service support portal where customers can open tickets and track resolution. Each customer administrator is provided login credentials to the support portal, allowing them to manage their issues from any device at any time. After a customer logs into the portal, the dashboard allows them to review incident tickets and their status, as well review reports that include: open tickets, closed tickets, and SLA reports to name a few.

Each ticket will be flagged with the user-selected category. These categories include urgency, symptom, and description, and allow for additional information or documentation to be included. After a category is selected, the user will submit the ticket for resolution.

Presidio Managed Services

Presidio Managed Services SDC is continuously available (24x7x365) with support channels available through web portal, email, and phone. Each support request automatically enters our Incident Management process where it is classified and prioritized. Our prioritization is a two-

step process where the business impact and the urgency (the extent to which the incident's resolution can bear delay) are evaluated with the customer's input.

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

Response:

AWS

Consequences/SLA remedies for failure to meet incident response and fix times associated with AWS cloud services are accessible online on AWS's website. Please refer to our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal."

Azure

Please refer to our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal." Additional information is accessible via the following link: https://azure.microsoft.com/en-us/support/legal/sla/summary/.

Presidio Managed Services

Presidio's Managed Services have Service Level Objectives (SLOs) that are specifically aligned to our ITIL-based incident management process, underlying incident priorities, and response times. Our SLOs do not have specific consequences by default but the underlying process includes an integrated escalation and notification procedures that ensures visibility of unresolved critical issues up through successive levels of the organization (including the Vice President of Operations) as an incident approaches the SLO. Presidio is willing to attach financial consequences to the SLOs if customers are interested.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Response:

AWS

AWS does not require systems to be brought offline to perform regular maintenance and system patching, and AWS's own maintenance and system patching generally do not impact customers. There may be occasions when AWS might schedule a customer instance for a reboot for necessary maintenance, such as to apply updates that require a reboot. No action is required on the customer's part; we recommend that customers wait for the reboot to occur within its scheduled window. These scheduled events are not frequent and if a customer instance will be affected by a scheduled event, they will receive an email prior to the scheduled event with details about the event, as well as a start and end date. Customers can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI. AWS will communicate with

customers, either via email, or through the AWS Service Health Dashboard if service use is likely to be adversely affected.

Azure

The majority of Azure services are highly available; each services availability information can be reviewed in the corresponding SLA (https://azure.microsoft.com/en-us/support/legal/sla/). For virtual machines, we recommend the use of availability sets/groups to limit or eliminate downtime. Additional information regarding availability sets and virtual machine maintenance is accessible via the following link: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/maintenance-and-updates.

Presidio Managed Services

Presidio Managed Services uses an ITIL-based Change Management process for planned downtime. The policy applies to the customer environments we support and the Presidio Managed Services operational environment.

The objectives of the Change Management Process are:

- To control changes to customer and Presidio systems through a process including documentation of the change being performed, approval of the change, implementation of the change, and testing the change after implementation.
- To provide an audit trail for traceability. This is to ensure we can tie the resolution of a customer or Presidio Incident to an implemented change. This process will also be used to track customer and Presidio upgrades to systems. This traceability is performed through documentation of the change, which includes a link from the Incident to the Change and vice versa, approval of the change, implementation of the change, and testing the change after implementation to ensure the Incident was resolved.
- To reduce service outages by performing changes to resolve issues before they occur, and to perform changes that are well planned and thoroughly tested after implementation.

Any changes made to a customer or Presidio Production environment must be logged through a Change Request. The type of Change Request a Change Owner selects will depend on which one best fits their situation regarding their change. Types of changes include:

- **Normal Change:** This is a change that is planned to be implemented within the designated Lead Times and is approved by the CAB if it impacts Presidio Managed Services. The majority of Presidio Managed Services changes should be Normal.
- **Standard Change:** This is a change that contains no to low risk, is very common so it is performed multiple times a day, and is easily reversible if it does need to be backed out. The majority of Presidio Standard Changes fall under the MACD category.

  Standard Changes must be implemented at least three times successfully with no issues as a Normal Change before they can be considered for Standard Change status. Once a Normal Change can meet these criteria, it can be proposed as a Standard Change.

- **Expedited Change:** This is a change that is a Normal except it must be implemented sooner than the designated Lead Times. Expedited Changes do require a justification for the faster than normal implementation date. If a justification is not provided, the Expedited Change will be rejected.
- **Emergency Change:** This is a change that requires it be implemented as soon as possible. These must be related to a high severity Incident (P1 or P2), requested item, or Problem. Emergency Changes may be logged after the high severity Incident (P1 or P2), requested item, or Problem is resolved. This prevents the Change Management Process from becoming a blocker to resolving the high severity event.

  If an Emergency Change is logged after the resolution of a high severity incident, it must be logged within 24 hours of the Incident Resolution. Approval of an after the fact Emergency Change is a validation that the Emergency Change was required at the time it was performed.
- **Unauthorized Change:** This is a change that was performed outside of logging a Change Request and did not receive any authorization before the work was performed. This Change Type is specifically requested by Change Management to log a change as record that it was performed without authorization. Unauthorized Changes must be logged within 24 hours of the request. All Unauthorized Changes will be reported to Senior Management of Managed Services.
- **Customer Maintenance Change:** This is a change that is being performed by an external customer where Presidio Managed Services is not performing the work. This Change Type is specifically entered by the Service Delivery Managers to suppress monitoring alerts during the customer maintenance period.

Change Approvals

All Change Requests must be authorized to the Scheduled state before they can be implemented. Each Change Type has a separate approval workflow, including:

- **Normal Approvals:** All Normal Change Requests must the following approvals before the change can be implemented:
  1. Tech Reviewer/Manager: This is a member of the department associated with the change. Either a peer or a Manager can approve the change at this level.
  2. Customer: Once the Tech Reviewer or Manager approves; a notification is sent to the Customer to approve. The e-mail the customer receives contains links for the customer to either approve or reject the Change Request.
  3. CAB: The CAB will only review and approve Normal Changes that are for internal Presidio changes or for customer changes they request to review. CAB approval will be captured outside of ServiceNow during the weekly CAB Meeting.
  4. Change Manager: Once the customer or CAB approves (depending on the Normal Change), the Change Manager reviews the Change Request to ensure everything is in

order and that it has the proper approvals. If everything is in order, then the Change Manager provides final approval.

- **Standard Approval**: There are no approvals required for Standard Changes that were pre-approved. All Standard Change Requests are processed through a Standard Change Template. Once the Template is populated and submitted, it is automatically approved for Implementation.
- If a Normal Change is being proposed to become a Standard Change, the proposal must be properly filled out and submitted in ServiceNow. All Standard Change proposals are reviewed and approved or rejected by the CAB and the Change Manager. If the proposal is approved, the proposal will be made into a new Standard Change Template. If the proposal is rejected, the person who proposed the change will be informed as to why it was rejected by the Change Manager.
- **Expedited Approval**: Expedited Changes follow the Normal Change Approval workflow. The only difference between an Expedited and Normal is the Expedited, with proper Justification, is allowed to be implemented within faster than normal lead times. If proper Justification for the Expedited request is not provided, the Expedited Change will be rejected.
- **Emergency Approval**: Emergency Changes have one approval level in the Emergency Change Advisory Board (ECAB). Only one member of the ECAB is required to approve an Emergency Change. If an Emergency Change does not provide the proper Justification for being submitted as an Emergency, it will be rejected.
- **Unauthorized Change**: Unauthorized Changes have one approval level in Change Management. Since Unauthorized Changes are after the fact requests, Change Management receives the request to approve to ensure the Change Request has all the proper details. Once Change Management approves an Unauthorized Change it is automatically closed.
- **Customer Maintenance Change**: Customer Maintenance Changes are similar to Standard Changes. Once the Change is submitted it is automatically approved. The Change moves into Implementation at the scheduled Start Time and is automatically Closed at the scheduled End Time.

Lead Times

Lead times is the amount of days that must be given from when a Change Request is submitted to when a Change Request is scheduled to be implemented. This provides the approvers time to review and justify the Change Request before providing their approval.

The Planned Start Date and Planned End Date fields on a Change Request must fall within the required lead time. If the Start and End dates do not fall within the required lead time (due to customer request, urgency, etc.), the Change Request will be automatically labeled as Expedited.

The Planned Start Date and Planned End Date are fixed dates. These are not placeholder dates for a Change Request. For example, if a Change Request has a Planned Start Date of January 1,

2016 at 8 PM that Change Request should never be implemented prior to January 1, 2016 at 8 PM. If a Change Request has a Planned End Date of January 1, 2016 at 9 PM, it is expected the Change Request will be finished no later than January 1, 2016 at 9 PM.

If the Planned Start or Planned End Dates need to be adjusted after the Change Request is submitted, the Change Request must be rescheduled. If a Change Request is implemented outside of the Planned Start Date or Planned End Date it will be marked with a Violation.

Lead times vary per Change Request type and include:

- Normal Changes: Normal Changes for external customers will require a 2-day lead time and will be required to be presented to CAB upon request.
- Normal Changes for internal customers (i.e. Presidio Managed Services) will require a 7 day lead time and must be presented to CAB.
- Standard Changes: Standard Changes do not have a required lead time.
- Expedited Changes: Expedited Changes do not have a required lead time. Expedited Changes are used in place of Normal Changes when a change must be implemented faster than the required lead time. Proper Justification is required to submit an Expedited Change.
- Emergency Changes: Emergency Changes do not have a required lead time.
- Unauthorized Changes: Unauthorized Changes do not have a required lead time.
- Customer Maintenance Changes: Customer Maintenance Changes do not have a required lead time.

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

Response:

AWS

Consequences/SLA remedies for failure to meet disaster recovery metrics associated with AWS cloud services are accessible online on AWS's website. Please refer to our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal."

Azure

Please refer to our previous response to RFP section 5.3.4 included in the document titled "Presidio Mandatory Minimums Response.pdf" uploaded in response to #2.1.3 in the SciQuest portal." Additional information is accessible via the following link: https://azure.microsoft.com/en-us/support/legal/sla/summary/.

Presidio Managed Services

Presidio's Managed Services have Service Level Objectives (SLOs) that are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number, complexity, and business impact of systems affected. Clients have the ability to set or change the priority level of an incident at any time, based on the impact to their specific business. Please refer to our previous responses to #8.10.2 in this section for additional information concerning priority levels and the corresponding service level parameters.

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.

Response:

AWS

The AWS Service Health Dashboard provides current and historical data online via AWS's website (http://status.aws.amazon.com/) across regions for each service offered. The status can be monitored in real time, or subscribed to as an RSS feed by service.

Current Status

AWS publishes up-to-the-minute information on service availability (Exhibit 6-14). Customers can check here to get current status information or subscribe to an RSS feed to be notified of interruptions to each individual service. If customers experience a real-time, operational issue with an AWS service that is not detailed in the current status, customers can inform AWS by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

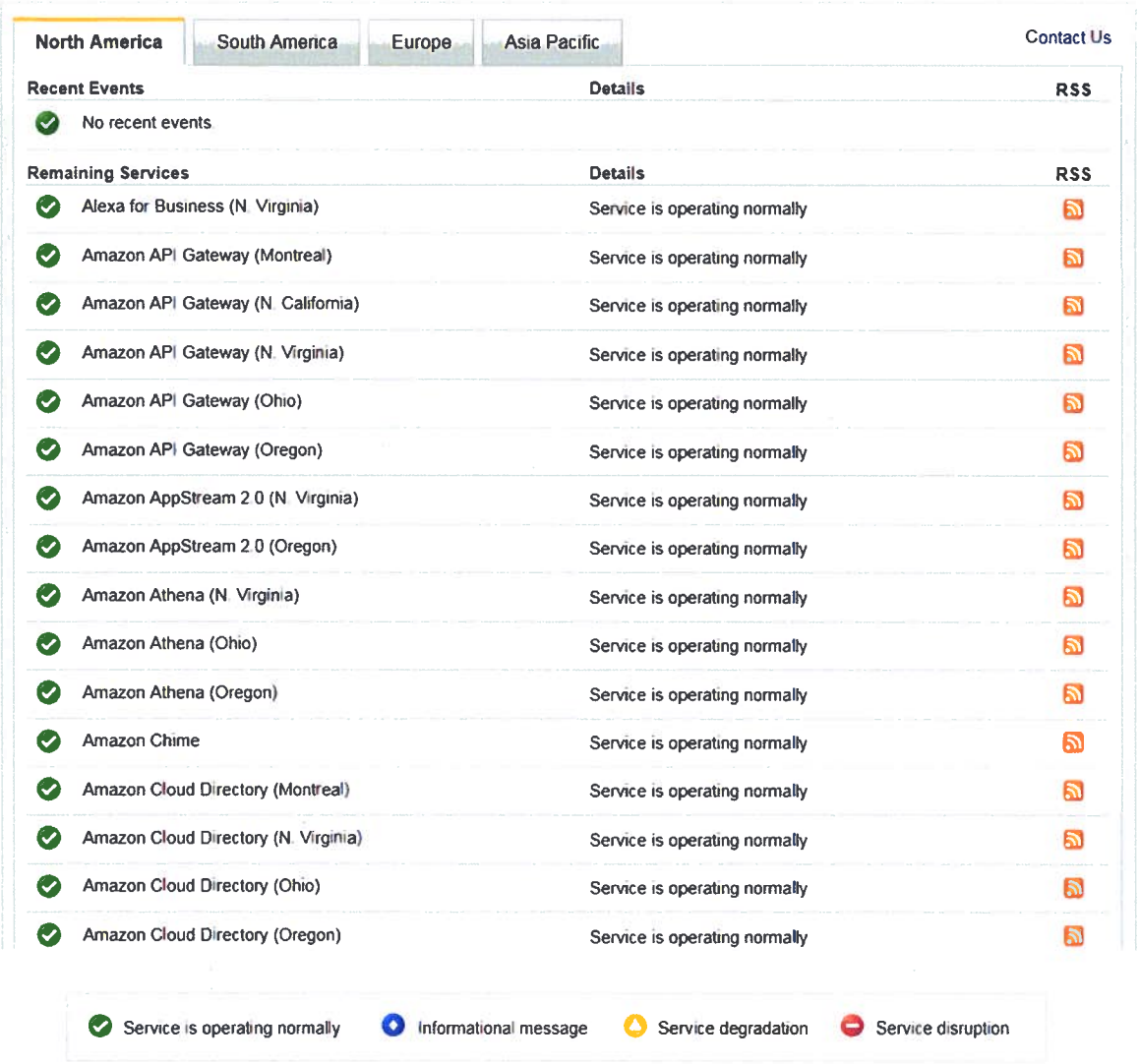


Exhibit 6-14. AWS Service Health Dashboard – Current Status

Status History

Amazon Web Services keeps a running log of all service interruptions that AWS publishes for the past year (Exhibit 6-15). Customers can mouse over any of the status icons to see a detailed incident report (click on the icon to persist the popup). Customers can click on the arrow buttons at the top of the table to move forward and backward through the calendar. All dates and times are Pacific Time (PST/PDT).

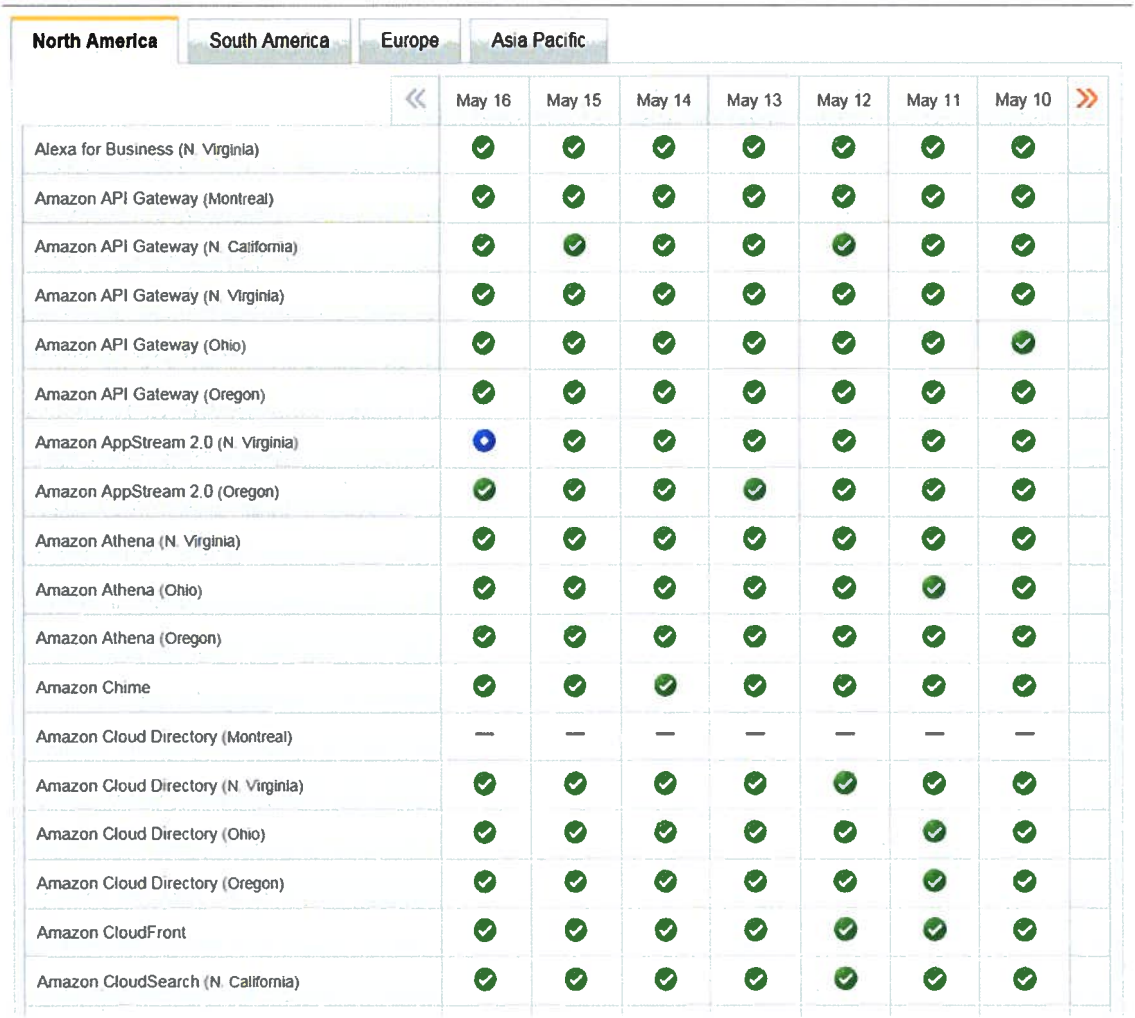


Exhibit 6-15. AWS Service Health Dashboard – Status History

Additionally, AWS customers can leverage AWS Cloud monitoring tools such as Amazon CloudWatch, AWS Trusted Advisor, AWS Health Checks, and third-party monitoring tools to extract metrics and system analytics.

Azure

Azure Status History reports are available via the web for 90 days (https://azure.microsoft.com/en-us/status/history/).

Presidio Managed Services

Presidio Managed Services includes a web-based Management Portal. The Client Portal is remotely accessible by clients and provides access to key information and services with respect to their managed services. The Client Portal capabilities include:

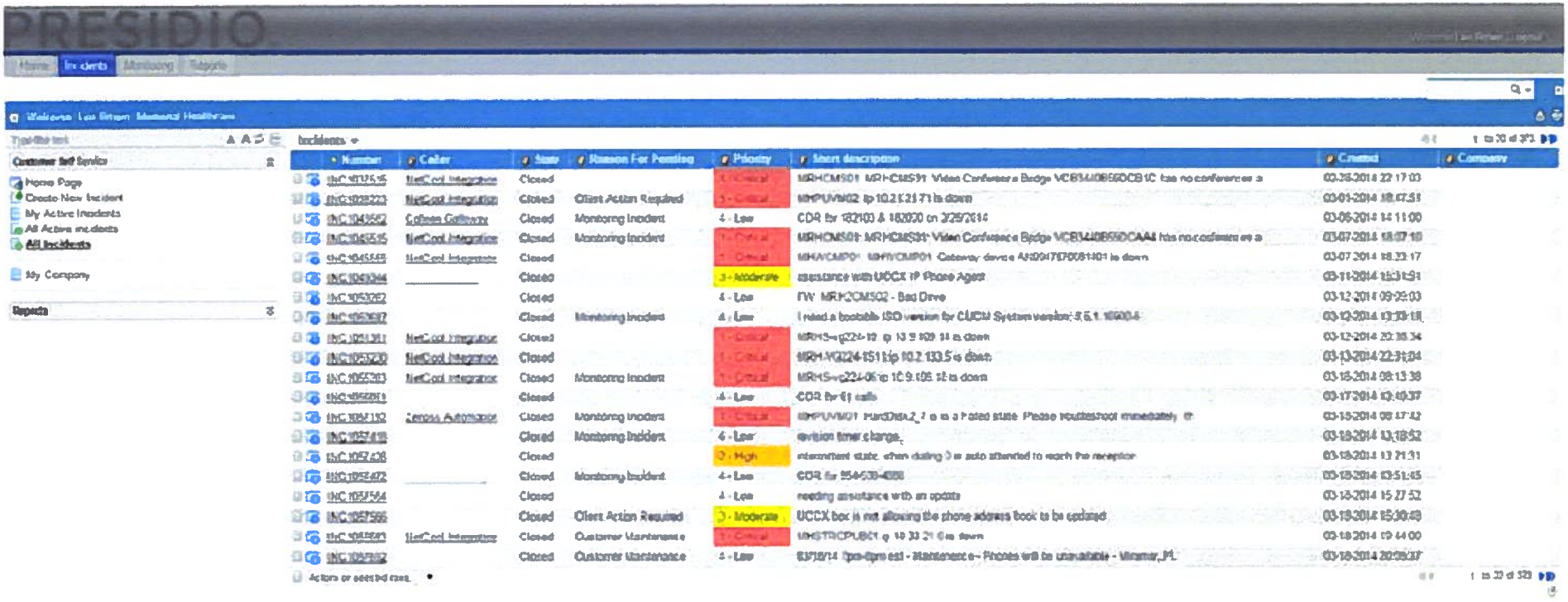
- Facilitating communication with the Presidio Service Desk, including request management.
- Viewing progress of service activities and the level of service being delivered.
- Viewing, creating, and updating incident tickets and change requests.
- Viewing status of managed and monitored-only CIs under contract.
- Generating reports for managed and monitored-only CIs under contract.

The Client Portal allows standard reports to be viewed and scheduled for automatic report delivery. The Client Portal also allows the Client to build reports based on monitored parameters; these can also be scheduled for automatic delivery. The screen shots included on the following pages provide sample reports from our Client Portal.

PRESIDIO

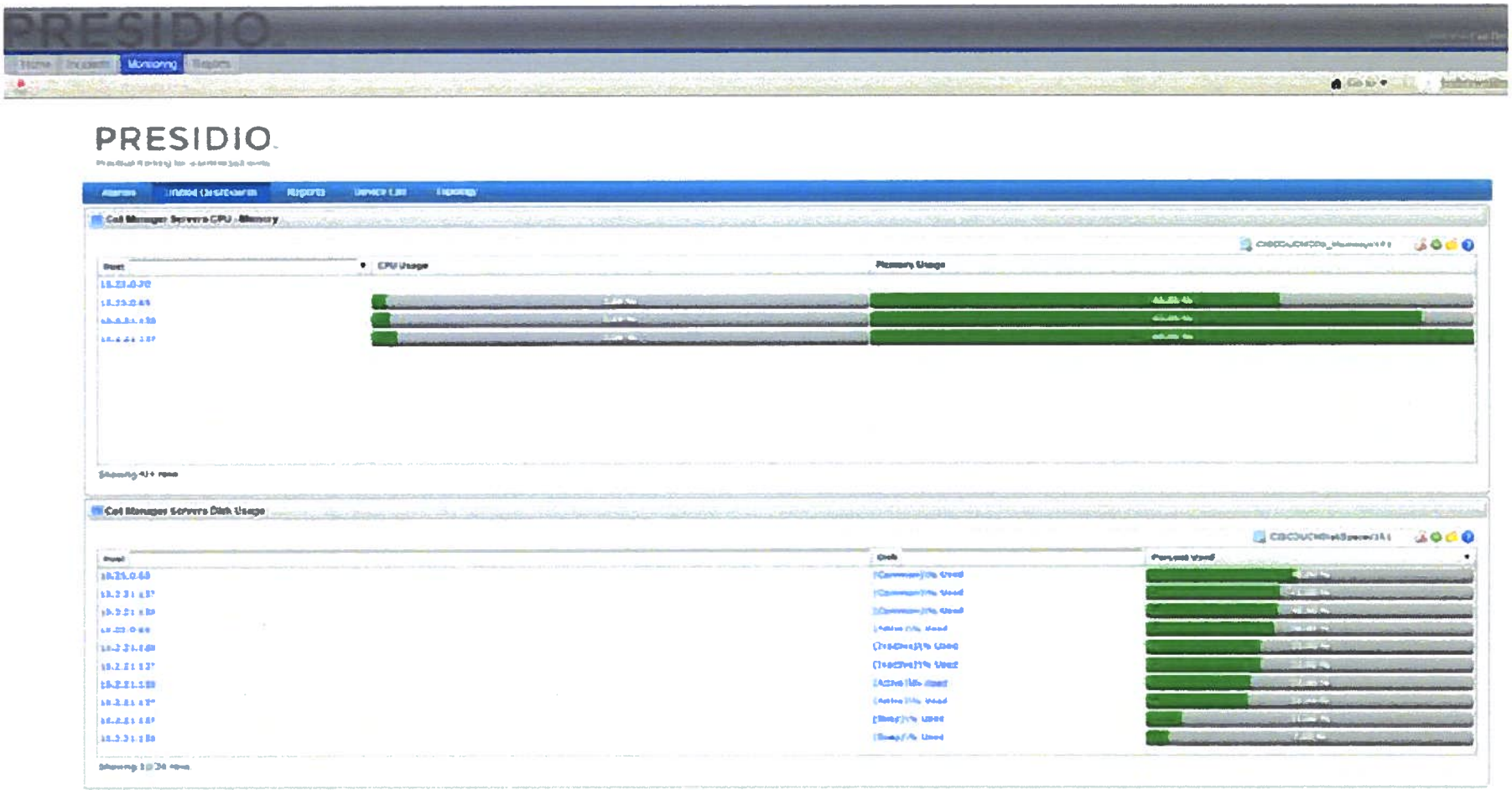
Sample Customer Portal: Incident Management

The customer may access a summary of incidents, including New, Client Action Required, Critical, and Resolved Incidents. The customer may create new tickets and see all previously created, open or closed.



PRESIDIO

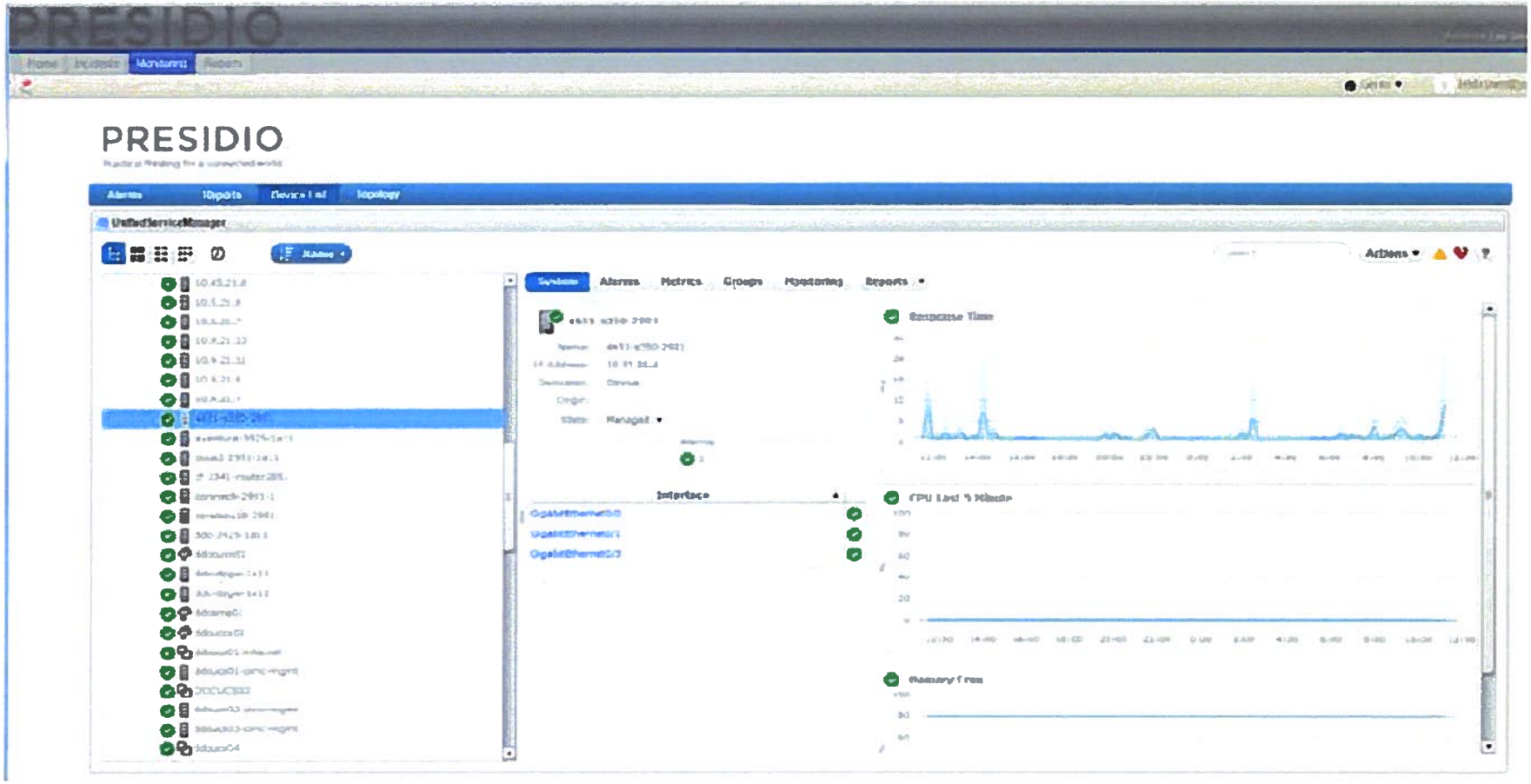
Sample Customer Portal: Top 10 Memory and Disk Space Usage Report



PRESIDIO

Sample Customer Portal Report: Performance by Device

The customer may select a device from their monitored devices to view Response Time, CPU, Free Memory, status of interfaces, Alarms & Metrics, and more.



PRESIDIO

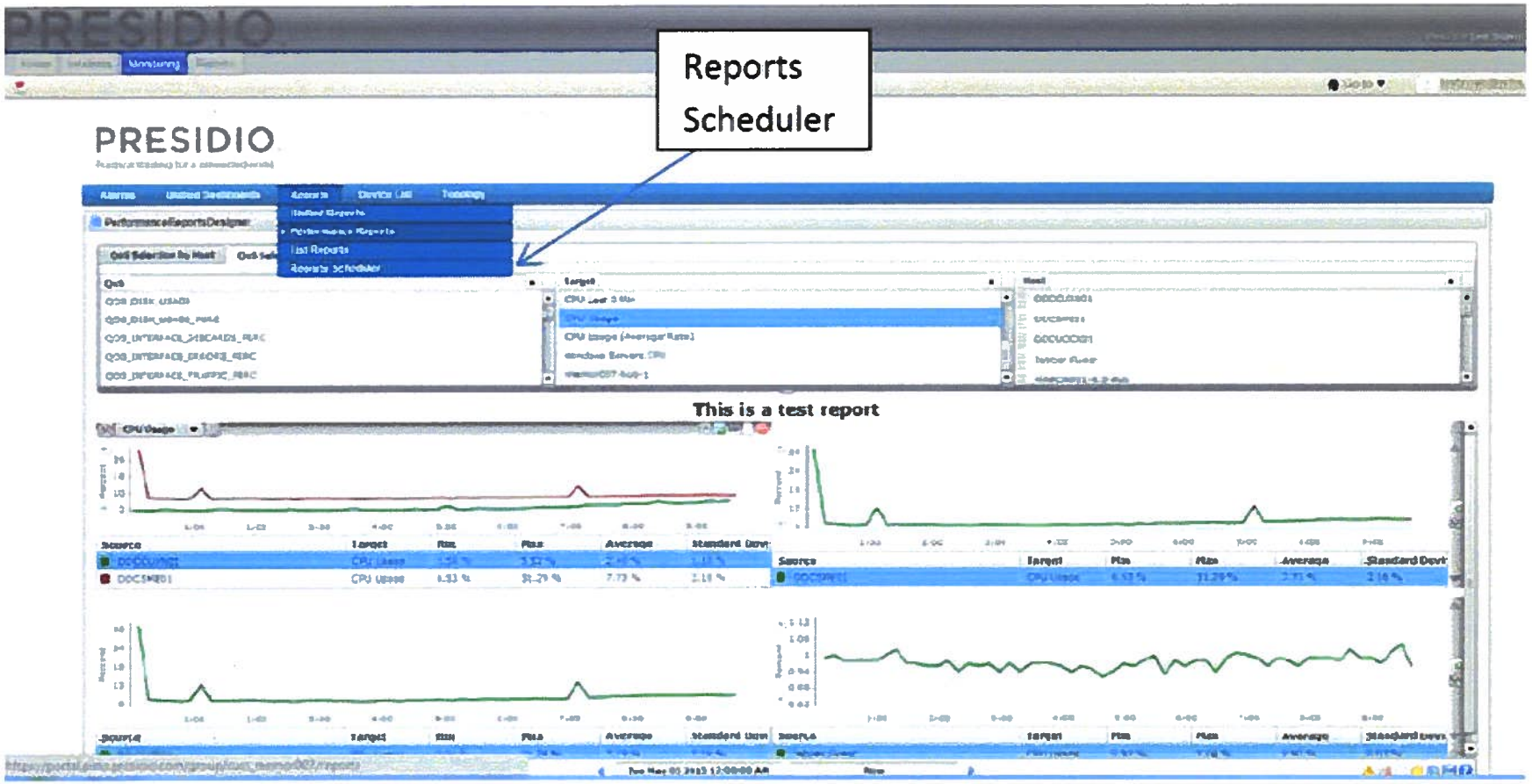
Sample Customer Portal Report: Performance Report Designer, CPU Usage by Hosts

The customer is able to customize reporting and manually select which hosts or devices are of interest for performance comparison.

PRESIDIO

Sample Customer Portal Report: Custom Report Scheduling

Custom reports may be scheduled for recurrent delivery to a specified email address in order to provide up-to-date performance statistics.

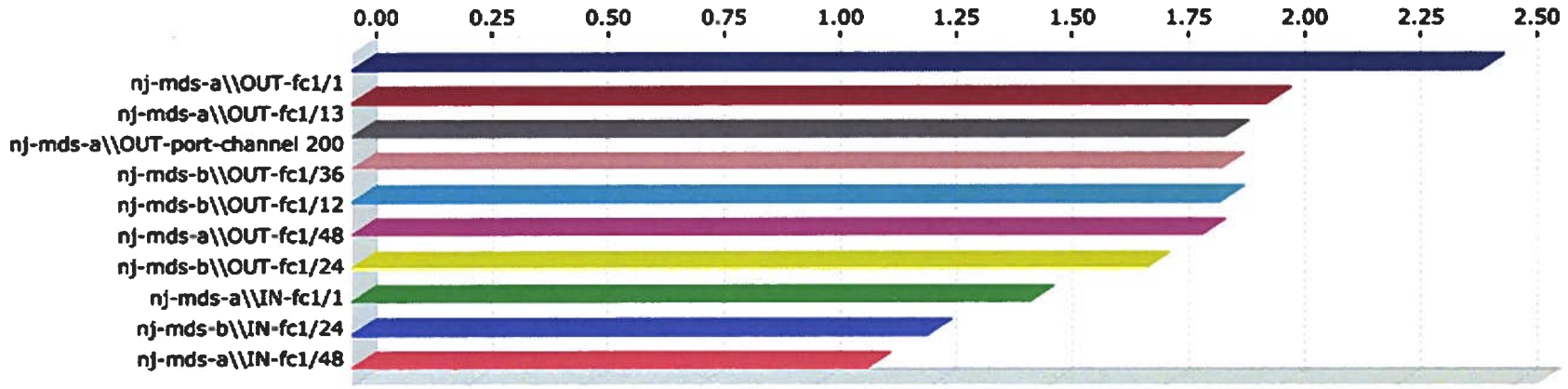


PRESIDIO

Sample Customer Portal Report: Utilization – Interface Bandwidth

Report Generated On: Tue Aug 30 12:27:27 EDT 2016

Report Excuted by: mbeard@presidio.com



Customer	Hostname	IP Address	Device Type	Interface	Business Impact	Bandwidth Avg (%)	Bandwidth Avg Rank	Bandwidth Max (%)	Bandwidth Max Rank
GAZZA001	nj-mds-a	10.172.100.33	Device	OUT-fc1/1	null	2.43	1	6.86	8
GAZZA001	nj-mds-a	10.172.100.33	Device	OUT-fc1/13	null	1.97	2	11.91	7
GAZZA001	nj-mds-a	10.172.100.33	Device	OUT-port-channel 200	null	1.88	3	16.60	6
GAZZA001	nj-mds-b	10.172.100.34	Device	OUT-fc1/36	null	1.87	4	21.75	1
GAZZA001	nj-mds-b	10.172.100.34	Device	OUT-fc1/12	null	1.87	5	18.40	5

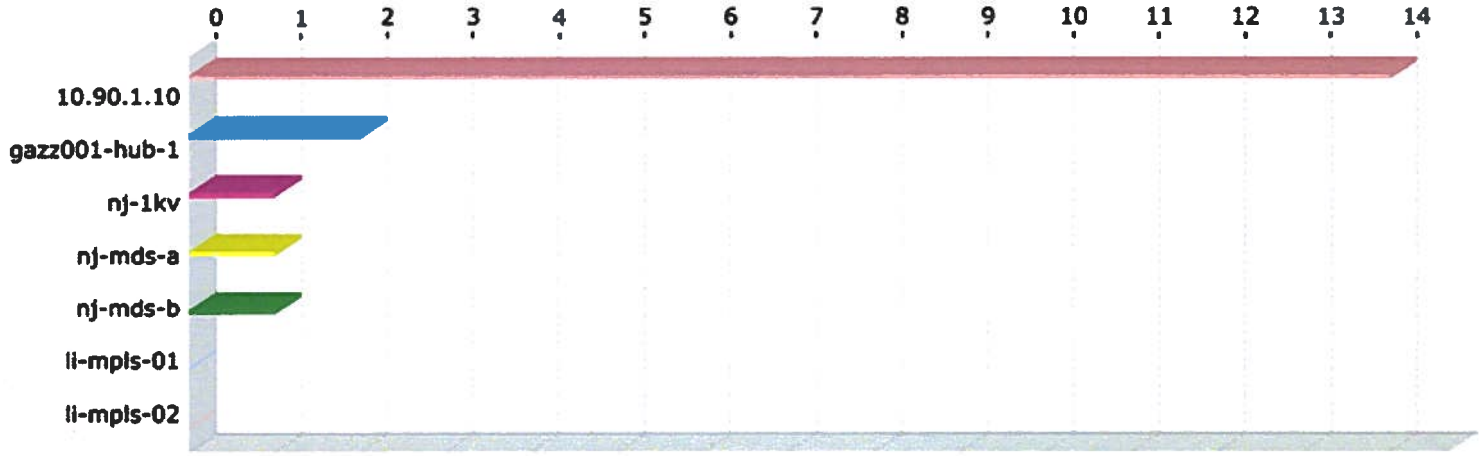
*Please note, Customer GAZZA001 is a demo account and not actual customer data

PRESIDIO

Sample Customer Portal Report: Utilization – Nimsoft – CPU

Report Generated On: Tue Aug 30 12:25:30 EDT 2016

Report Excuted by: mbeard@presidio.com



Customer	Hostname	IP Address	Device Type	Business Impact	CPU Avg (%)	CPU Avg Rank	CPU Max (%)	CPU Max Rank
GAZZA001	10.90.1.10	10.90.1.10	Device	null	14	1	62	1
GAZZA001	gazz001-hub-1	10.200.2.197	Host	null	2	2	11	5
GAZZA001	nj-1kv	10.172.100.35	Device	null	1	3	61	2
GAZZA001	nj-mds-a	10.172.100.33	Device	null	1	4	23	3
GAZZA001	nj-mds-b	10.172.100.34	Device	null	1	5	23	3

*Please note, Customer GAZZA001 is a demo account and not actual customer data

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

Response:

AWS

Please refer to the AWS capabilities of AWS CloudTrail, Amazon CloudWatch, and LogAnalyzer for Amazon CloudFront detailed in our previous response to #8.6.6 in this section.

Azure

Please refer to our previous response to #8.6.6 included in this section.

Presidio Managed Services

Presidio Managed Services includes a Web-based Management Portal. The Client Portal is remotely accessible by Clients and provides access to key information and services with respect to their managed services. Key capabilities of our Client Portal include:

- Facilitating communication with the Presidio Service Desk, including request management.
- Viewing progress of service activities and the level of service being delivered.
- Viewing, creating, and updating incident tickets and change requests.
- Viewing status of managed and monitored-only CIs under contract.
- Generating reports for managed and monitored-only CIs under contract. The web-based reports can also be printed through the web-based interface.

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

Response:

AWS

AWS Support is available 24x7x365 for all AWS cloud services offerings.

Azure

To the extent deliverable by the SLA, on demand deployment is supported 24x365.

Presidio Managed Services

Presidio Managed Services is continuously available (24x7x365) in each of its Service Delivery Centers to support any modifications to our client's infrastructure.

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

Response:

AWS

Auto Scaling allows customers to scale their Amazon EC2 capacity up or down automatically according to conditions that they define. Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their Amazon EC2 fleet or maintain their Amazon EC2 fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision Amazon EC2 capacity in advance. For example, customers can set a condition to add new Amazon EC2 instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the Amazon EC2 fleet goes above 70%; and similarly, customers can set a condition to remove Amazon EC2 instances in the same increments when CPU utilization falls below 10%.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables customers to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Customers can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS database instances, as well as custom metrics generated by applications and services and any log files applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep application running smoothly.

Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and ELB to dynamically deploy new instances on-demand as depicted in Exhibit 6-16.

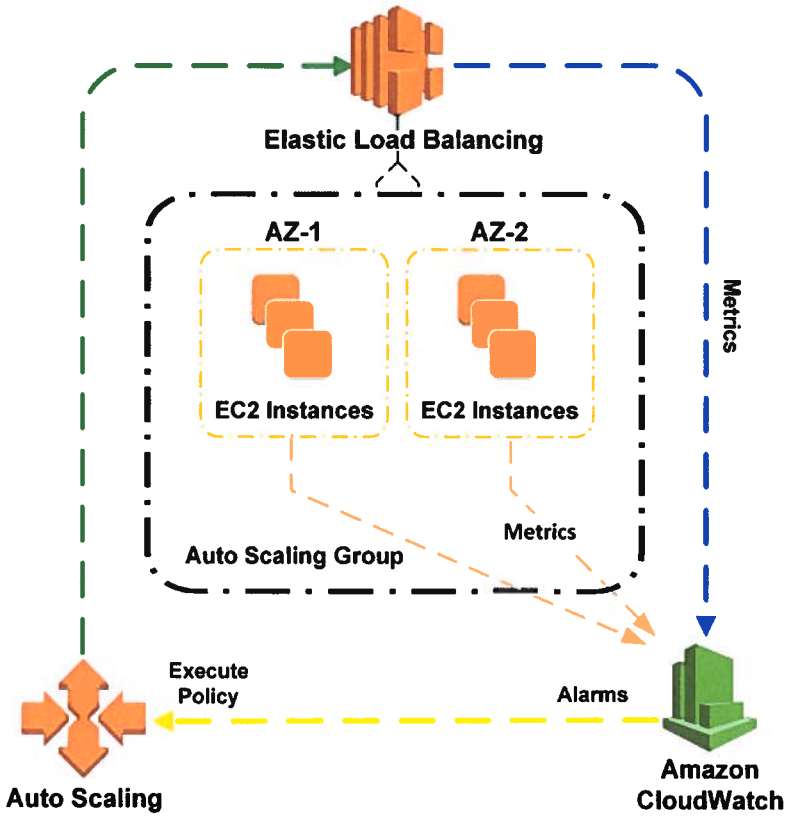


Exhibit 6-16. Auto Scaling with Elastic Load Balancing and Amazon CloudWatch Alarms

Azure

To the extent deliverable by the SLA, scaling up and down, as well as scaling in and out is supported 24x365.

Presidio Managed Services

Presidio Managed Services is continuously available (24x7x365) in each of our Service Delivery Centers to support any scale up or scale down changes introduced to our client's infrastructure.

8.13 (E) CLOUD SECURITY ALLIANCE

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)

b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)

c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)

d. Completion CSA STAR Continuous Monitoring. (5 points)

Response:

AWS

AWS has completed the CSA STAR Self-Assessment, which is accessible for download via the following link: https://cloudsecurityalliance.org/registry/amazon/.

AWS has completed the Exhibit 1 to Attachment B – CAIQ. Please refer to the document titled "Attachment 1 to Presidio Technical Response - AWS CAIQ.pdf" uploaded to the Supplier Attachments area in the SciQuest portal.

Per the CSA definitions, AWS aligns with the CSA STAR Attestation and Certification via the determinations in AWS's third-party audits for SOC and ISO:

> *"CSA STAR Level 2 Attestation is based on SOC2, which can be requested using AWS Artifact accessible via the following link: https://aws.amazon.com/artifact/. The SOC 2 report audit attests that AWS has been validated by a third-party auditor to confirm that AWS's control objectives are appropriately designed and operating effectively."*

As noted on the CSA website, CSA is still defining the Level 3 Continuous Monitoring requirements. Since AWS is unable to determine alignment for this reason, AWS does provide customers with the tools they need to meet continuous monitoring requirements. Customers can leverage the AWS Security by Design (SbD) program by providing control responsibilities outlines, the automation of security baselines, the configuration of security and the customer audit of controls for AWS customer infrastructure, operating systems, services and applications running in AWS. This standardized, automated, prescriptive and repeatable design can be deployed for common use cases, security standards and audit requirements across multiple industries and workloads. For more information, please refer to the following link. https://aws.amazon.com/compliance/security-by-design/.

Azure

Microsoft publishes both a CAIQ and a CCM-based report for Microsoft Azure. Please refer to the documents titled "Attachment 2 to Presidio Technical Response – Azure CAIQ.xlxs," and "Attachment 3 to Presidio Technical Response – Azure CCM.pdf," uploaded to the Supplier Attachments area in the SciQuest portal.

Microsoft Azure has completed a CSA STAR Attestation. Please refer to the document titled "Attachment 4 to Presidio Technical Response – Azure CSA STAR Attestation.pdf" uploaded to the Supplier Attachments area in the SciQuest portal.

Microsoft Azure has attained Cloud Security Management System - CSA STAR Certification 2014 (Certificate Number: STAR 658377 Expiry Date: 2020-06-19). Please refer to the document titled "Attachment 5 to Presidio Technical Response – Azure CSA STAR Certification.pdf" uploaded to the Supplier Attachments area in the SciQuest portal.

Azure's CCM responses are scoped to Azure services in alignment with ISO 27001 and PCI DSS attestations. Azure validates services using third-party penetration testing based upon the Open

Web Application Security Project (OWASP) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices.

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.

Response:

Presidio offers a white glove service for emergency provisioning and rush orders. The escalation process begins with our dedicated Inside Sales Cloud Specialist, Donna Bodrogi. Purchasing Entities requiring emergency or rush provisioning can contact the ISR in two ways, directly by phone at the number listed, or via email. If through email, the subject line should indicate "Rush Order Service Required".

The ISR initiates the process by assigning the request to the regionally based Account Manager responsible for assisting the Purchasing Entity through the provisioning and order process.

If required, the Purchasing Entity can also escalate to our dedicated Contract Manager, Bret Gessner.

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

Response:

AWS and Azure

Most SaaS/IaaS/PaaS solutions have a provision time of a few seconds to several minutes on AWS and Azure; however, the magnitude of services such as large data ingests into the cloud may take several hours and depend on the magnitude of the workloads. Several solutions feature scripting and packaged deployment options with the goal of increasing automation and minimizing the lead time for provisioning.

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.

Response:

AWS

AWS customers control the entire lifecycle of their content, and manage their content in accordance with their own specific needs and/or legal requirements, including content classification, access control, retention, and deletion.

Azure

Azure customers control the entire lifecycle of their content, and manage their content in accordance with their own specific needs and/or legal requirements, including content classification, access control, retention, and deletion.

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

Response:

AWS

AWS disaster recovery risks depend on the recovery architecture selected. As such, AWS infrastructure has a high level of availability and provides customers with the features needed to deploy a resilient IT architecture. Its systems are designed to tolerate system or hardware failures with minimal customer impact. The AWS Cloud supports many popular disaster recovery architectures, ranging from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. All data centers are online and serving customers; no data center is "cold." In the case of a failure, automated processes move data traffic away from the affected area. By distributing applications across multiple AWS Availability Zones, customers can remain resilient in the face of most failure modes, including natural disasters or system failures. Customers can build highly resilient systems in the cloud by employing multiple instances in multiple AWS Availability Zones and using data replication to achieve extremely high recovery time and recovery point objectives. Customers are responsible for managing and testing the backup and recovery of the information system that is built on the AWS infrastructure. Customers can use the AWS infrastructure to enable faster disaster recovery of critical IT systems without incurring the infrastructure expense of a second physical site.

Azure

Information on Azure disaster recovery features is accessible via the following link: https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications.

As with availability considerations, Azure provides resiliency technical guidance designed to support disaster recovery. There is also a relationship between availability features of Azure and disaster recovery. For example, the management of roles across fault domains increases the availability of an application. Without that management, an unhandled hardware failure would become a "disaster" scenario. Leveraging these availability features and strategies is an important part of disaster-proofing a customer's application.

Multiple Data Center Regions

Azure maintains data centers in many regions around the world. This infrastructure supports several disaster recovery scenarios, such as system-provided geo-replication of Azure Storage to secondary regions. Customers can also easily and inexpensively deploy a cloud service to

multiple locations around the world. Customers can compare this with the cost and difficulty of building and maintaining their own data centers in multiple regions. Deploying data and services to multiple regions helps protect applications from a major outage in a single region. As customers design their disaster recovery plan, it's important to understand the concept of paired regions. Additional information is accessible via the following link: https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions.

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.

Response:

AWS

The AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where AWS has multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.

AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage accessible via the following link: https://aws.amazon.com/about-aws/global-infrastructure/. Exhibit 6-17 depicts the current AWS Regions and Availability Zones, along with the four new regions AWS has announced plans for.

The AWS products and services that are available in each region are listed at the Region Table webpage accessible via the following link: https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/.

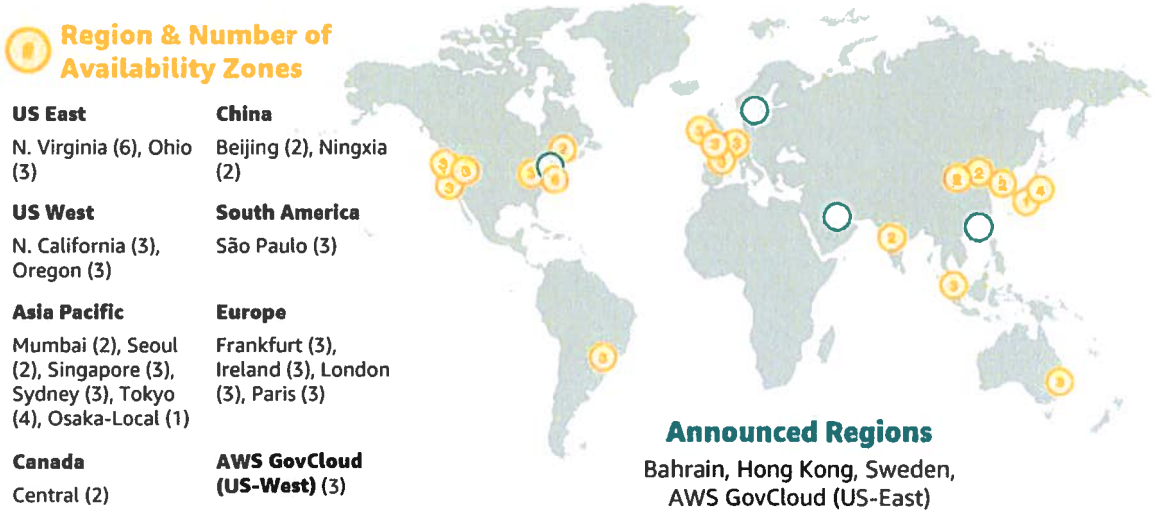


Exhibit 6-17. Global Map of AWS Regions and Availability Zones

Exhibit 6-18 illustrates the relationship between AWS regions and Availability Zones.

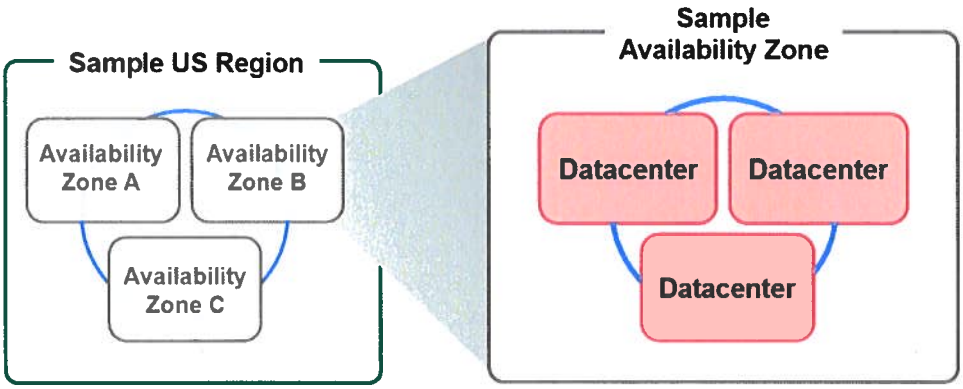


Exhibit 6-18. AWS Regions and Availability Zones

Azure

Microsoft Azure has 50 regional data centers across 140 countries with large-scale redundant and geo-redundant failover capabilities. Additional information is accessible via the following link: https://azure.microsoft.com/en-us/global-infrastructure/regions/.

8.16 (E) HOSTING AND PROVISIONING

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

Response:

AWS

The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Customers can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS Regions and allows customers to provision resources across multiple regions.

Azure

Microsoft Azure Provisioning is an automated process that allows interaction from the Azure Portal or completely remote using Azure APIs, as a single example virtual machine in just a few minutes in the Azure portal. The normal steps taken are planning for the deployment, selecting the VM image, creating the VM, and then managing the virtual machine. The VM image can be from the images available from the gallery, including Windows and Linux, and the processes supports customized images from a customer's on-premise standard image template library. This process can be repeated one at a time or automated with PowerShell to create hundreds of Virtual Machines at one time. This example is for automating a VM; however, all of the properties in Microsoft Azure can be automated using the same methods, through the portal or PowerShell. Other examples for automating include Cloud Storage, SQL Servers, and Virtual Networks.

8.16.2 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).*

Response:

AWS

AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS

Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools.

The AWS Developer Tools helps customers securely store and version control their application's source code and automatically build, test, and deploy applications to AWS or their on-premises environment.

Deploying New Servers

AWS tools include:

- **AWS Marketplace** is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses. AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. Visitors to AWS Marketplace can use 1-Click deployment to quickly launch pre-configured software and pay only for what they use, by the hour or month. AWS handles billing and payments, and software charges appear on customers' AWS bill.
- **AWS Console/Compute:** EC2 servers provide several options and optimization to run client workloads.
- **AWS CodeCommit:** A fully-managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories. AWS CodeCommit eliminates the need to operate a source control system or worry about scaling its infrastructure. Customers can use AWS CodeCommit to securely store anything from source code to binaries, and it works seamlessly with existing Git tools.
- **AWS CodePipeline:** A continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. AWS CodePipeline builds, tests, and deploys a customer's code every time there is a code change, based on the release process models they define. This enables customers to rapidly and reliably deliver features and updates. Customers can easily build out an end-to-end solution by using our pre-built plugins for popular third-party services like GitHub or integrating custom plugins into any stage of the release process. With AWS CodePipeline, customers only pay for what they use. There are no upfront fees or long-term commitments.
- **AWS CodeBuild:** A fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, customers don't need to provision, manage, and scale their own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue. Customers can get started quickly by using prepackaged build environments, or they can create custom build environments that use their own build tools. With AWS CodeBuild, customers are charged by the minute for the compute resources they use.

Creating and Storing Server Images

AWS tools include:

- **AWS CodeDeploy:** A service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for customers to rapidly release new features, helps them avoid downtime during application deployment, and handles the complexity of updating their applications. Customers can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service also scales with infrastructure so customers can easily deploy to one instance or thousands.
- **Management Tools:** AWS provides a broad set of services that help IT administrators, systems administrators, and developers more easily manage and monitor their resources. Using these fully managed services, customers can automatically provision, configure, and manage their AWS or on-premises resources at scale. Customers can also monitor infrastructure logs and metrics using real-time dashboards and alarms. AWS also helps customers monitor, track, and enforce compliance and security.

Securing Additional Storage Space

AWS tools include:

- **AWS CloudFormation:** Gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application.
- **AWS Service Catalog:** Allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.

Configuration Management

AWS tools include:

- **AWS OpsWorks:** A configuration management service that helps customers configure and operate applications of all shapes and sizes using Chef. Customers can define the application's architecture and the specification of each component including package installation, software configuration, and resources such as storage. Customers can start from templates for common technologies like application servers and databases or build their own to perform any task that can be scripted. AWS OpsWorks includes automation

to scale applications based on time or load and dynamic configuration to orchestrate changes as an environment scales.

- **AWS Systems Manager:** Allows customers to centralize operational data from multiple AWS services and automate tasks across AWS resources. Customers can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, customers can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central place to view and manage AWS resources, so customers can have complete visibility and control over their operations.

Governance and Compliance

AWS tools include:

- **AWS Config: A** fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config Rules enables customers to create rules that automatically check the configuration of AWS resources recorded by AWS Config. With AWS Config, customers can discover existing and deleted AWS resources, determine their overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.
- **AWS CloudTrail:** A web service that records AWS API calls for a customer's account and delivers log files to them. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service. With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS Cloud services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.
- **AWS Service Catalog:** Allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.

Monitoring Tools

AWS tools include:

- **Amazon CloudWatch:** A monitoring service for AWS Cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon Relational Database Service (Amazon RDS) DB instances, as well as custom metrics generated by the customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health and then use those insights to react and keep their application running smoothly.
- **AWS Trusted Advisor:** An online resource to help customers reduce cost, increase performance, and improve security by optimizing their AWS environment. AWS Trusted Advisor provides real-time guidance to help customers provision their resources following AWS best practices.

Azure

Deploying new servers, and creating and storing server images for multiple deployments, is accomplished using a web-based Management Portal, Azure Resource Manager, PowerShell commandlets, or an API using one of the provided SDKs. The Azure Portal provides the flexibility to create one or thousands of Virtual Machines (VMs). A single VM can be created, and two or more VMs can be created and placed into an "availability set" so the uptime SLA is applied. The Azure Portal and the underlining Azure APIs are used to extend or scale systems easily.

The addition of cloud storage can be automated using the Azure Portal or PowerShell. Azure Blob storage is a service that stores file data in the cloud. Blob storage can store any type of text or binary data, such as a document, media file, or application installer. Blob storage is sometimes referred to as object storage. Azure Blob storage can be completely automated using .NET, Node.js, Java, C++, PHP, Ruby, Python, IOS, and Xamarin.

Monitoring cloud services are included in the Azure Portal and available from APIs in the Azure portal and on the individual VM available through the Operating System. Customers can monitor key performance metrics for cloud services in the Azure classic portal. Customers can set the level of monitoring to minimal and verbose for each service role, and can customize the monitoring displays. Monitoring displays in the Azure classic portal are highly configurable. Customers can choose the metrics they want to monitor in the metrics list on the Monitor page, and can choose which metrics to plot in the metrics charts on the Monitor page and the dashboard.

By default, minimal monitoring is provided for a new cloud service using performance counters gathered from the host operating system for the roles instances (virtual machines). The minimal

metrics are limited to CPU Percentage, Data In, Data Out, Disk Read Throughput, and Disk Write Throughput. By configuring verbose monitoring, customers can receive additional metrics based on performance data within the virtual machines (role instances). The verbose metrics enable closer analysis of issues that occur during application operations.

By default, performance counter data from role instances is sampled and transferred from the role instance at 3-minute intervals. When verbose monitoring is enabled, the raw performance counter data is aggregated for each role instance and across role instances for each role at intervals of 5 minutes, 1 hour, and 12 hours. The aggregated data is purged after 10 days.

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

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

Response:

Presidio offers a range of testing phases based on the type of development, migration, or specific solution. The testing phase of a project can range from a few days to months depending on factors such as the size and complexity of the project. Training and knowledge transfer options also vary based on the type of project.

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Response:

Presidio technical resources will determine the requirements for a proof of concept (POC) evaluation and create a vision deck that details the budget, duration, technology stack, timeline, and related information. We will assess the POC design against client requirements and any compliance criteria to ensure alignment with larger project initiatives. POC development can proceed on the cloud in the client environment whereby the client can use appropriate data loads to test the solution's viability. We will use the feedback gathered from the POC output in support of the final project requirements.

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

Response:

Presidio ensures client satisfaction and that program objectives are met in order to enable customer success. Enabling customers to use innovative solutions is critical and we provide the following no-cost training and support:

- Project knowledge transfer, including:
  - Technical solution overviews, and
  - FAQ session.
- Documentation review.
- Customer training session(s), as agreed upon in the project Statement of Work (SOW).

8.18 (E) INTEGRATION AND CUSTOMIZATION

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Response:

Our proposed cloud solutions can be integrated with other applications via the following solutions based on the appropriate design:

- API-based integration.
- Web application/portal integration.
- Database synchronization.

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

Response:

Presidio utilizes its deep engineering pool and pedigree to approach each project on a case-by-case basis. Each project begins with our Pre-Sales Solutions Architect (SA) discussing the project goals and objectives with the Purchasing Entity. The SA then creates a high-level design, a Bill of Materials, and a Statement of Work. After the Purchasing Entity approves the project scope, our Project Management team engages our delivery engineers and holds internal and external kickoff meetings to launch the project. The Project Management team spearheads the project with regularly scheduled meetings to ensure the project is running within scope and all teams are updated on the status.

8.19 (E) MARKETING PLAN

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

Response:

Presidio understands that award of a Master Agreement and Participating Addendums alone will not guarantee business. We realize our responsibility and the importance of communicating our contracted cloud solutions and services to the market. Through properly planned marketing campaigns, we are confident we can generate business and success for the NASPO ValuePoint Cloud Solutions program. We have demonstrated our marketing expertise effectively with other contract vehicles and we are well known for driving attendance to our customer events and seminars; becoming a go-to partner with our CSPs for these types of initiatives.

Presidio conducts significant business with SLED clients nationwide. One of our primary goals will be to educate these customers on the benefits of using the NASPO ValuePoint Cloud Solutions program and to drive as much business as possible through this contract. Our geographic presence in 60+ offices strategically located throughout the U.S. enables us to support the Master Agreement and Participating Addendums with nationwide coverage for sales,

marketing, and technical support. We will call upon our experience with existing contract vehicles and leverage our current customer base as a foundation. With our coverage model, expertise, and existing customer base, we will continue our growth momentum and bring new business through this contract.

Our customer engagement model is a high-touch, local presence focusing on value-based solutions. Our marketing plan aligns with this approach through in-market educational seminars on Presidio's cloud solutions that present specific workload use cases for SLED customers to consume and detail how they can leverage the NASPO Cloud contract. Our national marketing team will lead our efforts to market the NASPO ValuePoint Cloud Solutions contracts through webinars to educate clients on platform offerings and how to source these types of services through NASPO. Our marketing plan may encompass outbound calling campaigns, advertising, clinics, seminars, demonstration facilities, and trade shows to present our cloud solutions offerings and services under this contract to potential customers. We also advertise in various trade publications. Additionally, our corporate website will include a dedicated NASPO ValuePoint Cloud Solutions web page featuring the latest information and access to program documentation.

Presidio views this contract opportunity as a strategic vehicle for continued success in bringing new solutions to our clients. We are confident we will continue substantial momentum and penetration in our SLED vertical with our cloud solution offerings.

8.20 (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.

Response:

Cloud solutions help businesses create agile, efficient IT environments that serve as a springboard for change. Presidio helps clients take cloud strategy and adoption to the next level. By closely aligning our services and solutions with our strategic CSP partners, our advanced cloud solutions practice offers cloud strategy, architecture, and implementation services along with application rationalization and migration across the hybrid and multi-cloud data center environment. Rather than a "one size fits all" approach, or having to choose between public or private, Presidio tailors hybrid solutions to meet clients' unique business requirements. We help our clients accelerate and simplify cloud adoption across the entire IT lifecycle.

PRESIDIO CLOUD CAPABILITIES

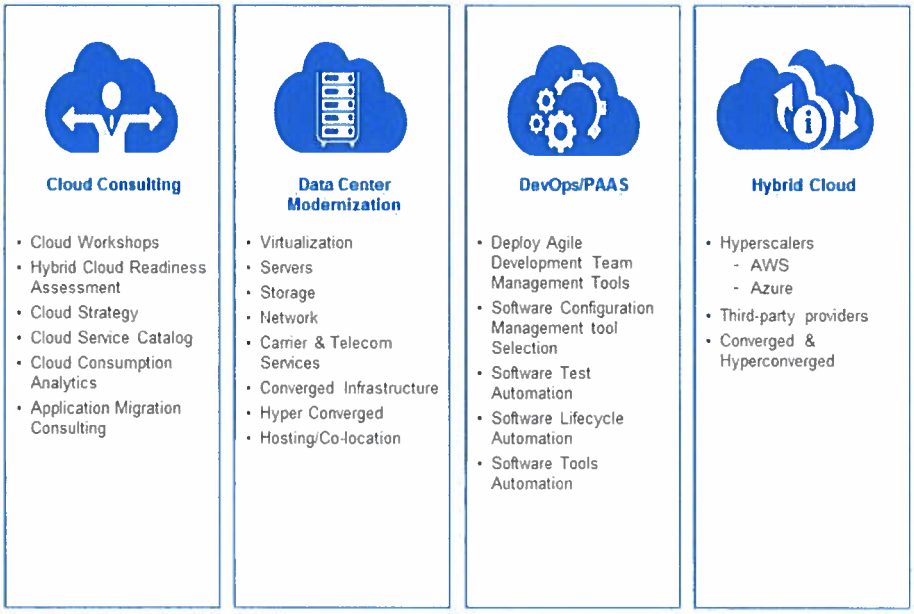


Exhibit 6-19. Presidio's Extensive Cloud Value-Added Services and Capabilities

Presidio cloud experts focus on advising, architecting, and implementing solutions that enable our customers to derive maximum value from their cloud investments. Our value-added services and cloud capabilities include:

- **Cloud Consulting**: Presidio offers Cloud Workshops that focus on customers' business drivers, processes, and technology. Our Hybrid Cloud Readiness Assessment offers customers the ability to evaluate their applications, services, software, and infrastructure for cloud readiness. During this assessment, we use our tools and services to look at services dependencies, QoS, SLA, security, costing, etc., and offer our customers a unique roadmap that shows them their cloud adoption readiness not just on technology but also on people/process. Cloud Consumption Analytics looks at two key factors, namely cost and risk for Cloud. If we decide that an application can be migrated, then we offer Application Migration Consulting and Services as well.
- **Data Center Modernization**: The public cloud is compelling customers to evaluate their current data centers. This includes upgrading and modernizing their data center with virtualization, faster servers/storage, and investments in new technologies like Hyper-Converged.
- **DevOps/PAAS**: Our software development team helps our customers with Agile Development and Software Tools Automation.

- Hybrid/Multi Cloud: We have an impressive set of hybrid/multi cloud capabilities and services encompassing consulting, design, integration, and migration associated with multiple CSP partners. Our cloud consulting and integration teams have deep-domain knowledge with a multitude of cloud technologies from industry leaders. Our focus is to architect the optimal solution to leverage both private and public cloud resources, and to integrate the right cloud solution that will deliver scalable, secure, high performing service delivery models for our clients.

Presidio provides our customers with lifecycle support for the cloud project, including design, migration, operation, and optimization. Presidio has the specialized resources to support the unique requirements of our SLED customers, and provide a consistent and effective engagement across cloud adoption.

8.22 (E) SUPPORTING INFRASTRUCTURE

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

Response:

Any infrastructure requirements to support the compute, storage, networking, and security pillars on the public cloud will be determined by Presidio based on project requirements. As such, certain design considerations will minimize the need for any new infrastructure. For all cloud solution projects, Presidio will perform an extensive analysis to determine what service(s) the client infrastructure can support before making appropriate recommendations.

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

Response:

The responsibility for any new infrastructure installation costs typically falls to the client; however, Presidio will provide a Statement of Work that details the budget and professional services required to complete necessary tasks while providing any relevant documentation.

AWS PUBLIC SECTOR ACCESS POLICY
(Last Updated April 2, 2018)

This AWS Public Sector Access Policy ("**Access Policy**") is hereby made a part of the agreement (the "**Agreement**") between [____INSERT END CUSTOMER NAME____] ("**Customer**") and [___INSERT SOLUTION PROVIDER NAME___] ("**Solution Provider**") regarding Customer's use of and access to the AWS Services via the AWS accounts provided to Customer by Provider ("**Solution Provider Accounts**"). Section 7 contains definitions of capitalized terms.

1. Scope. This Access Policy is not an agreement with Amazon Web Services, Inc. ("**AWS**"). It sets out the rules, conditions, and restrictions that apply to Customer's use of the AWS Services under Solution Provider Accounts where (1) Customer does not have an AWS Services Agreement with AWS; or (2) if Customer does have an AWS Services Agreement with AWS, Solution Provider has not designated it to AWS as Customer's own account under the AWS Solution Provider Program.

2. Use of the Services.

2.1 Generally. Solution Provider gives Customer access to the AWS Services via Solution Provider Accounts, and Customer's use of and access to the AWS Services is governed by the Agreement and this Access Policy. Contractual commitments by AWS to Solution Provider (for example, service level agreements) do not apply as between Customer and AWS. Customer must look solely to Solution Provider under this Agreement regarding any claims or damages relating to, or arising out of, the AWS Services. Solution Provider is not an agent of AWS and is not acting on behalf of AWS, and Customer is not a third party beneficiary of any agreement between Solution Provider and AWS.

2.2 Disclaimers; Limitations on AWS Liability. THE AWS SERVICES, AWS CONTENT, AND THIRD-PARTY CONTENT ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, NEITHER AWS, NOR SOLUTION PROVIDER ON BEHALF OF AWS, MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT. AWS DISCLAIMS ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (a) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (c) THAT THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (d) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST, ALTERED, OR DAMAGED. AWS WILL NOT BE LIABLE TO CUSTOMER FOR ANY DAMAGES OF ANY KIND (INCLUDING DIRECT, INDIRECT, INCIDENTIAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, DAMAGES FOR LOST PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA, THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY CUSTOMER IN CONNECTION WITH CUSTOMER'S USE OF THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT) ARISING IN CONNECTION WITH, OR RELATED TO, CUSTOMER'S INABILITY TO USE THE AWS SERVICES, INCLUDING AS A RESULT OF ANY TERMINATION OR SUSPENSION OF SOLUTION PROVIDER ACCOUNTS UNDER ANY AGREEMENT BETWEEN AWS AND SOLUTION PROVIDER, DISCONTINUATION OR DOWNTIME OF AWS SERVICES, OR ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ACCOUNT CONTENT.

2.3 Account Keys. Solution Provider may provide Customer with AWS account keys which will allow Customer to directly access the AWS Services via Solution Provider Accounts. AWS is not responsible to Customer for any activities that occur under these account keys, regardless of whether the activities are undertaken by Customer, Solution Provider, or a third party (including Customer employees, contractors or agents) and AWS is not responsible to Customer for unauthorized access to Solution Provider Accounts.

2.4 Third-Party Content. Through the use of the AWS Services or the AWS Site, Customer may have access to Third-Party Content, which is made available directly to Customer by other entities or individuals under separate terms and conditions, including separate fees and charges. Customer's use of any Third-Party Content is at its sole risk.

2.5 AWS Services Policies. All access to and use of AWS Services is subject to the AWS Services Policies. (Notwithstanding anything in the Acceptable Use Policy and AWS Service Terms, these two AWS Services Policies are not separate agreements between Customer and AWS.)

2.6 Customer Responsibilities. Unless otherwise agreed by Solution Provider, Customer is solely responsible for the development, content, operation, maintenance, and use of Account Content in Solution Provider Accounts, including (a) the technical operation of AWS Services in connection with Account Content; (b) compliance of Account Content with the AWS Services Policies and applicable law; (c) any action Customer permits, assists, or facilitates any other person or entity to take under Solution Provider Accounts; and (d) use of AWS Services or Account Content by End Users under Solution Provider Accounts (and ensuring that End Users comply with Customer obligations under this Access Policy). If Customer becomes aware of any violation of its obligations under this Access Policy caused by itself or an End User, Customer will immediately terminate such End User's access to Account Content and the AWS Services by such End User. Unless otherwise agreed by Solution Provider, Customer is solely responsible for properly configuring and using the AWS Services and otherwise taking appropriate action to secure, protect, and backup Solution Provider Accounts and Account Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Account Content from unauthorized access and routinely archiving Account Content.

3. AWS Services Interruption. AWS may suspend the Solution Provider Accounts used by Customer to access the AWS Services immediately if AWS determines Customer's or an End User's use of the AWS Services (i) violates the AWS Services Policies; (ii) poses a security risk to the AWS Services or any other AWS customer, (iii) may harm AWS systems or the systems or Content of any other AWS customer; or (iv) may subject AWS to liability as a result of any of the foregoing. We will provide notice of any suspension to Solution Provider, who is solely responsible for providing any notices to Customer under the Agreement. Nothing in this Section 3 will operate to limit Customer's rights or remedies otherwise available to Customer against Solution Provider under the Agreement or applicable law.

4. Transition of Solution Provider Accounts. Except as otherwise provided by law or the Agreement, a transition of Solution Provider Accounts from Solution Provider to a third party (or directly to AWS) requires advance written consent by Solution Provider (which Solution Provider must also obtain from AWS). Customer agrees to cooperate with Solution Provider in transitioning Solution Provider Accounts, and to provide all appropriate information and take all appropriate action necessary to facilitate such transition. In any case, absent prior authorization by AWS, Customer may not transfer Solution Provider Accounts to other providers that are not authorized to resell AWS Services.

5. Proprietary Rights

5.1 Generally. AWS or its licensors own all right, title, and interest in and to the AWS Services, and all related technology and intellectual property rights. Customer (a) has the right to access and use the AWS Services under Solution Provider Accounts solely in accordance with this Access Policy and the Agreement, and (b) may copy and use the AWS Content provided by Solution Provider (or, as applicable, by AWS) solely in connection with Customer's permitted use of the AWS Services. Except as provided in this Section 5, Customer obtains no rights under this Access Policy from AWS, its affiliates, or Solution Provider to the AWS Services, the AWS Content, or Third-Party Content, including any related intellectual property rights. Some AWS Content and Third-Party Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, or other open source license. By using those materials, Customer is subject to such additional terms. Customer is solely responsible for securing any necessary approvals for the download and use of such materials.

5.2 Restrictions. Neither Customer nor any End User will use the AWS Services or AWS Content in any manner or for any purpose other than as expressly permitted by this Access Policy and the Agreement. Neither Customer nor any End User will, or will attempt to (a) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any AWS Content or Content included in the AWS Services (except to the extent Content included in the AWS Services is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the AWS Services or apply any other process or procedure to derive the source code of any software included in the AWS Services (except to the extent applicable

law doesn't allow this restriction), or (c) access or use the AWS Services in a way intended to avoid incurring fees or exceeding usage limits or quotas.

5.3 Suggestions. If Customer provides any Suggestions to AWS or its affiliates, AWS and its affiliates will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions and agrees to provide Customer and AWS any assistance required to document, perfect, and maintain AWS's rights in the Suggestions.

5.4 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the AWS Services are provided (as applicable) as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the AWS Services. If Customer is using the AWS Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Customer will immediately discontinue its use of the AWS Services (including any AWS Content).

6. Representations and Warranties. Customer represents and warrants to Solution Provider that (a) Customer's and its End Users' use of the AWS Services (including any use by its employees, personnel, and (except for Solution Provider) contractors) will not violate this Access Policy, including the AWS Services Policies; (b) Customer or its licensors own all right, title, and interest in and to Account Content; (c) Account Content (including the use, development, design, production, advertising, or marketing of Account Content) or the combination of Account Content with other applications, Content, or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) Customer's use of the AWS Services will not cause harm to any End User.

7. Definitions.

"Account Content" means Content that Customer or any End User (a) runs on the AWS Services, (b) causes to interface with the AWS Services, or (c) uploads to the AWS Services or otherwise transfer, process, use or store in connection with the AWS Services.

"AWS Content" means Content AWS makes available (either directly or indirectly) in connection with the AWS Services or on the AWS Site to allow or facilitate access to and use of the AWS Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the AWS Services.

"AWS Services" means, collectively or individually (as applicable), the web services made commercially available by us to Solution Provider for use under this Access Policy, including (as applicable) those web services described in the AWS Service Terms.

"AWS Services Agreement" means the AWS Customer Agreement at http://aws.amazon.com/agreement, or other written agreement by and between AWS and Customer (if any) governing Customer's access to and use of the AWS Services.

"AWS Services Policies" means the following provisions (uses of the pronoun "you" shall refer to Customer):

- *AWS Acceptable Use Policy*, located at http://aws.amazon.com/aup (as it may updated by AWS from time to time), which describes prohibited uses of the AWS Services and the AWS Site;
- *AWS Service Terms,* located at http://aws.amazon.com/serviceterms (as they may be updated by AWS from time to time), which include the rights and restrictions for particular AWS Services;
- *AWS Site Terms*, located at http://aws.amazon.com/terms/ (as they may be updated by AWS from time to time), which govern the use of the AWS Site; and
- All restrictions described in the AWS Content and on the AWS Site.

"AWS Site" means http://aws.amazon.com and any successor or related site designated by AWS.

"Content" means software (including machine images), data, text, audio, video or images.

"Documentation" means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at http://aws.amazon.com/documentation, as such documentation may be updated by us from time to time.

"End Customer Account" means an AWS account designated as such under the AWS Solution Provider Program, through which AWS Services are provided by Solution Provider to Customer, and in connection with which AWS and Customer have an AWS Services Agreement.

"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Account Content; or (b) otherwise accesses or uses the AWS Services under Solution Provider Accounts. The term "End User" does not include individuals or entities when they are accessing or using the AWS Services or any Content under their own AWS account, rather than Solution Provider Accounts.

"Solution Provider Accounts" means Solution Provider's AWS accounts through which AWS Services are provided by Solution Provider to Customer.

"Suggestions" means all suggested improvements to the AWS Services or AWS Content that Customer provides to AWS or its affiliates.

"Third-Party Content" means Content made available to Customer by any third party on the AWS Site or in conjunction with the AWS Services.

Microsoft Volume Licensing

Microsoft Cloud Agreement

This Microsoft Cloud Agreement is entered into between the entity you represent, or, if you do not designate an entity in connection with a Subscription purchase or renewal, you individually ("Customer"), and Microsoft Corporation ("Microsoft"). It consists of the terms and conditions below, Use Rights, SLA, and all documents referenced within those documents (together, the "agreement"). It is effective on the date that your Reseller provisions your Subscription. Key terms are defined in Section 10.

1. Grants, rights and terms.

All rights granted under this agreement are non-exclusive and non-transferable and apply as long as neither Customer nor any of its Affiliates is in material breach of this agreement.

a. Software. Upon acceptance of each order, Microsoft grants Customer a limited right to use the Software in the quantities ordered.

(i) Use Rights. The Use Rights in effect when Customer orders Software will apply to Customer's use of the version of the Software that is current at the time. For future versions and new Software, the Use Rights in effect when those versions and Software are first released will apply. Changes Microsoft makes to the Use Rights for a particular version will not apply unless Customer chooses to have those changes apply.

(ii) Temporary and perpetual licenses. Licenses available on a subscription basis are temporary. For all other licenses, the right to use Software becomes perpetual upon payment in full.

b. Online Services. Customer may use the Online Services as provided in this agreement.

(i) Online Services Terms. The Online Services Terms in effect when Customer orders or renews a subscription to an Online Service will apply for the applicable subscription term. For Online Services that are billed periodically based on consumption, the Online Services Terms current at the start of each billing period will apply to usage during that period.

(ii) Suspension. Microsoft may suspend use of an Online Service during Customer's violation of the Acceptable Use Policy or failure to respond to a claim of alleged infringement. Microsoft will give Customer notice before suspending an Online Service when reasonable.

(iii) End Users. Customer controls access by End Users, and is responsible for their use of the Product in accordance with this agreement. For example, Customer will ensure End Users comply with the Acceptable Use Policy.

(iv) Customer Data. Customer is solely responsible for the content of all Customer Data. Customer will secure and maintain all rights in Customer Data necessary for Microsoft to provide the Online Services to Customer without violating the rights of any third party or otherwise obligating Microsoft to Customer or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to Customer's use of the Product other than as expressly set forth in this agreement or as required by applicable law.

(v) Responsibility for your accounts. Customer is responsible for maintaining the confidentiality of any non-public authentication credentials associated with Customer's use of the Online Services. Customer must promptly notify customer support about any possible misuse of Customer's accounts or authentication credentials or any security incident related to the Online Services.

c. **License transfers.** License transfers are not permitted, except that Customer may transfer only fully-paid perpetual licenses to (1) an Affiliate or (2) a third party, solely in connection with the transfer of hardware or employees to whom the licenses have been assigned to the third party as part of (a) a divestiture of all or part of an Affiliate or (b) a merger involving Customer or an Affiliate. Upon such transfer, Customer and its Affiliates must uninstall and discontinue using the licensed Product and render any copies unusable. Attempted license transfers that do not comply with this agreement are void.

d. **Reservation of rights.** Products are protected by copyright and other intellectual property rights laws and international treaties. Microsoft reserves all rights not expressly granted in this agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use Software on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

e. **Restrictions.** Customer may use the Product only in accordance with this agreement. Customer may not (and is not licensed to): (1) reverse engineer, decompile or disassemble any Product or Fix, or attempt to do so; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (3) work around any technical limitations in a Product or Fix or restrictions in Product documentation. Customer may not disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters Customer's use of the Online Services. Except as expressly permitted in this agreement or Product documentation, Customer may not distribute, sublicense, rent, lease, lend, resell or transfer and Products, in whole or in part, or use them to offer hosting services to a third party.

f. **Preview releases.** Microsoft may make Previews available. **Previews are provided "as-is," "with all faults," and "as-available," and are excluded from the SLA and all limited warranties provided in this agreement.** Previews may not be covered by customer support. Previews may be subject to reduced or different security, compliance, and privacy commitments, as further explained in the Online Services Terms and any additional notices provided with the Preview. Microsoft may change or discontinue Previews at any time without notice. Microsoft also may choose not to release a Preview into "General Availability."

g. **Verifying compliance for Products.**

(i) **Right to verify compliance.** Customer must keep records relating to all use and distribution of Products by Customer and its Affiliates. Microsoft has the right, at its expense, to verify compliance with the Products' license terms. Customer must promptly provide any information reasonably requested by the independent auditors retained by Microsoft in furtherance of the verification, including access to systems running the Products and evidence of licenses for Products that Customer hosts, sublicenses, or distributes to third parties. Customer agrees to complete Microsoft's self-audit process, which Microsoft may request as an alternative to a third party audit.

(ii) **Remedies for non-compliance.** If verification or self-audit reveals any unlicensed use of Products, then within 30 days (1) Customer must order sufficient licenses to cover its use, and (2) if unlicensed use is 5% or more, Customer must reimburse Microsoft for the costs Microsoft incurred in verification and acquire the necessary additional licenses at 125% of the price, based on the then-current price last and customer price level. The unlicensed use percentage is based on the total number of licenses purchased for current use compared to the actual installed base. If there is no unlicensed use, Microsoft will not subject Customer to another verification for at least one year. By exercising the rights and procedures described above, Microsoft does not waive its rights to enforce this agreement or to protect its intellectual property by any other legal means.

(iii) **Verification process.** Microsoft will notify Customer at least 30 days in advance of its intent to verify Customers' compliance with the license terms for the Products Customer

and its Affiliates use or distribute. Microsoft will engage an independent auditor, which will be subject to a confidentiality obligation. Any information collected in the self-audit will be used solely for purposes of determining compliance. This verification will take place during normal business hours and in a manner that does not unreasonably interfere with Customer's operations.

2. *Subscriptions, ordering.*

a. **Choosing a Reseller.** Customer must choose and maintain a Reseller authorized within its region. If Microsoft or Reseller chooses to discontinue doing business with each other, Customer must choose a replacement Reseller or purchase a Subscription directly from Microsoft, which may require Customer to accept different terms.

b. **Available Subscription offers.** The Subscription offers available to Customer will be established by its Reseller and generally can be categorized as one or a combination of the following:

(i) **Online Services Commitment Offering.** Customer commits in advance to purchase a specific quantity of Online Services for use during a Term and to pay upfront or on a periodic basis for continued use of the Online Service.

(ii) **Consumption Offering (also called Pay-As-You-Go).** Customer pays based on actual usage with no upfront commitment.

(iii) **Limited Offering.** Customer receives a limited quantity of Online Services for a limited term without charge (for example, a free trial) or as part of another Microsoft offering (for example, MSDN). Provisions in this agreement with respect to the SLA and data retention may not apply.

(iv) **Software Commitment Offering.** Customer commits in advance to purchase a specific quantity of Software for use during a Term and to pay upfront or on a periodic basis for continued use of the Software.

c. **Ordering.**

(i) Orders must be placed through Customer's designated Reseller. Customer may place orders for its Affiliates under this agreement and grant its Affiliates administrative rights to manage the Subscription, but, Affiliates may not place orders under this agreement. Customer also may assign the rights granted under Section 1.a and 1.b to a third party for use by that third party in Customer's internal business. If Customer grants any rights to Affiliates or third parties with respect to Software or Customer's Subscription, such Affiliates or third parties will be bound by this agreement and Customer agrees to be jointly and severally liable for any actions of such Affiliates or third parties related to their use of the Products.

(ii) Customer's Reseller may permit Customer to modify the quantity of Online Services ordered during the Term of a Subscription. Additional quantities of Online Services added to a Subscription will expire at the end of that Subscription.

d. **Pricing and payment.** Prices for each Product and any terms and conditions for invoicing and payment will be established by Customer's Reseller.

e. **Renewal.**

(i) Upon renewal of a Subscription, Customer may be required to sign a new agreement, a supplemental agreement or an amendment to this agreement.

(ii) Customer's Subscription will automatically renew unless Customer provides its Reseller with notice of its intent not to renew prior to the expiration of the Term.

f. **Eligibility for Academic, Government and Nonprofit versions.** Customer agrees that if it is purchasing an academic, government or nonprofit offer, Customer meets the respective eligibility requirements listed at the following sites:

(i) For academic offers, the requirements for educational institutions (including administrative offices or boards of education, public libraries, or public museums) listed at http://go.microsoft.com/academic;

(ii) For government offers, the requirements listed at http://go.microsoft.com/government; and

(iii) For nonprofit offers, the requirements listed at http://go.microsoft.com/nonprofit.

Microsoft reserves the right to verify eligibility at any time and suspend the Online Service if the eligibility requirements are not met.

g. **Taxes.** The parties are not liable for any of the taxes of the other party that the other party is legally obligated to pay and which are incurred or arise in connection with or related to the transactions contemplated under this agreement, and all such taxes will be the financial responsibility of the party who is obligated by operation of law to pay such tax.

3. *Term, termination.*

a. **Agreement term and termination.** This agreement will remain in effect until the expiration or termination of Customer's Subscription, whichever is earliest. Customer may terminate this agreement at any time by contacting its Reseller. The expiration or termination of this agreement will only terminate Customer's right to place new orders for additional Products under this agreement.

b. **Termination for cause.** If either party breaches this Agreement, the other party may terminate the breached agreement (in whole or in part, including orders) upon notice. If the breach is curable within 30 days, then the terminating party must provide 30 days' notice to the breaching party and an opportunity to cure the breach.

c. **Cancel a Subscription.** Customer's Reseller will establish the terms and conditions, if any, upon which Customer may cancel a Subscription.

4. *Security, privacy, and data protection.*

a. **Reseller Administrator Access and Customer Data.** Customer acknowledges and agrees that (i) once Customer has chosen a Reseller, that Reseller will be the primary administrator of the Online Services for the Term and will have administrative privileges and access to Customer Data, however, Customer may request additional administrator privileges from its Reseller; (ii) Customer can, at its sole discretion and at any time during the Term, terminate its Reseller's administrative privileges; (iii) Reseller's privacy practices with respect to Customer Data or any services provided by Reseller are subject to the terms of Customer's agreement with its Reseller and may differ from Microsoft's privacy practices; and (iv) Reseller may collect, use, transfer, disclose, and otherwise process Customer Data, including personal data. Customer consents to Microsoft providing Reseller with Customer Data and information that Customer provides to Microsoft for purposes of ordering, provisioning and administering the Online Services.

b. Customer consents to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. Customer may choose to provide personal information to Microsoft on behalf of third parties (including your contacts, resellers, distributors, administrators, and employees) as part of this agreement. Customer will obtain

all required consents from third parties under applicable privacy and data protection laws before providing personal information to Microsoft.

c. Additional privacy and security details are in the Online Services Terms. The commitments made in the Online Services Terms only apply to the Online Services purchased under this agreement and not to any services or products provided by a Reseller. If Customer uses software or services that are hosted by a Reseller, that use will be subject to Reseller's privacy practices, which may differ from Microsoft's.

d. As and to the extent required by law, Customer shall notify the individual users of the Online Services that their data may be processed for the purpose of disclosing it to law enforcement or other governmental authorities as directed by Reseller or as required by law, and Customer shall obtain the users' consent to the same.

e. Customer appoints Reseller as its agent for purposes of interfacing with and providing instructions to Microsoft for purposes of this Section 4.

5. *Warranties.*

a. **Limited warranty.**

(i) **Software.** Microsoft warrants that each version of the Software will perform substantially as described in the applicable Product documentation for one year from the date Customer is first licensed for that version. If it does not, and Customer notifies Microsoft within the warranty term, then Microsoft will, at its option, (1) return the price Customer paid for the Software license or (2) repair or replace the Software.

(ii) **Online Services.** Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's use. Customer's remedies for breach of this warranty are in the SLA.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any breach of warranty claims not made during the warranty period.

b. **Exclusions.** The warranties in this agreement do not apply to problems caused by accident, abuse or use inconsistent with this agreement, including failure to meet minimum system requirements. These warranties do not apply to free or trial products, Previews, Limited Offerings, or to components of Products that Customer is permitted to redistribute.

c. **Disclaimer. Except for the limited warranties above, Microsoft provides no warranties or conditions for Products and disclaims any other express, implied, or statutory warranties for Products, including warranties of quality, title, non-infringement, merchantability and fitness for a particular purpose.**

6. *Defense of third party claims.*

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

a. **By Microsoft.** Microsoft will defend Customer against any third-party claim to the extent it alleges that a Product or Fix made available by Microsoft for a fee and used within the scope of the license granted under this agreement (unmodified from the form provided by Microsoft

and not combined with anything else), misappropriates a trade secret or directly infringes a patent, copyright, trademark or other proprietary right of a third party. If Microsoft is unable to resolve a claim of infringement under commercially reasonable terms, it may, as its option, either: (1) modify or replace the Product or fix with a functional equivalent; or (2) terminate Customer's license and refund any prepaid license fees (less depreciation on a five-year, straight-line basis) for perpetual licenses and any amount paid for Online Services for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product or Fix after being notified to stop due to a third-party claim.

b. **By Customer.** To the extent permitted by applicable law, Customer will defend Microsoft against any third-party claim to the extent it alleges that: (1) any Customer Data or non-Microsoft software hosted in an Online Service by Microsoft on Customer's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Customer's use of any Product or Fix, alone or in combination with anything else, violates the law or harms a third party.

7. *Limitation of liability.*

For each Product, each party's maximum, aggregate liability to the other under this agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Products during the term of this agreement, subject to the following:

a. **Online Services.** For Online Services, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Online Service during the 12 months before the incident; provided that in no event will Microsoft's aggregate liability for any Online Service exceed the amount paid for that Online Service during the Subscription.

b. **Free Products and distributable code.** For Products provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US$5,000.

c. **Exclusions. In no event will either party be liable for loss of revenue or indirect, special, incidental, consequential, punitive, or exemplary damages, or damages for loss of use, lost profits, revenues, business interruption, or loss of business information, however caused or on any theory of liability.**

d. **Exceptions.** The limits of liability in this section apply to the fullest extent permitted by applicable law, but do not apply to: (1) the parties' obligations under section 6; or (2) violation of the other's intellectual property rights.

8. *Support and Professional Services.*

Customer's Reseller will provide details on support services available for Products purchased under this agreement. Support services may be performed by Reseller or its designee, which in some cases may be Microsoft. If Customer purchases Professional Services under this agreement, the performance of those Professional Services will be subject to the terms and conditions in the Use Rights.

9. *Miscellaneous.*

a. **Notices.** You must send notices by mail, return receipt requested, to the address below.

Notices should be sent to:
Microsoft Corporation Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329

You agree to receive electronic notices from us, which will be sent by email to the account administrator(s) named for your Subscription. Notices are effective on the date on the return receipt or, for email, when sent. You are responsible for ensuring that the email address for the account administrator(s) named for your Subscription is accurate and current. Any email notice that we send to that email address will be effective when sent, whether or not you actually receive the email.

b. **Assignment.** You may not assign this agreement either in whole or in part. Microsoft may transfer this agreement without your consent, but only to one of Microsoft's Affiliates. Any prohibited assignment is void.

c. **Severability.** If any part of this agreement is held unenforceable, the rest remains in full force and effect.

d. **Waiver.** Failure to enforce any provision of this agreement will not constitute a waiver.

e. **No agency.** This agreement does not create an agency, partnership, or joint venture.

f. **No third-party beneficiaries.** There are no third-party beneficiaries to this agreement.

g. **Use of contractors.** Microsoft may use contractors to perform services, but will be responsible for their performance, subject to the terms of this agreement.

h. **Microsoft as an independent contractor.** The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's confidential information.

i. **Agreement not exclusive.** Customer is free to enter into agreements to license, use or promote non-Microsoft products or services.

j. **Applicable law and venue.** This agreement is governed by Washington law, without regard to its conflict of laws principles, except that (i) if you are a U.S. Government entity, this agreement is governed by the laws of the United States, and (ii) if you are a state or local government entity in the United States, this agreement is governed by the laws of that state. Any action to enforce this agreement must be brought in the State of Washington. This choice of jurisdiction does not prevent either party from seeking injunctive relief in any appropriate jurisdiction with respect to violation of intellectual property rights.

k. **Entire agreement.** This agreement is the entire agreement concerning its subject matter and supersedes any prior or concurrent communications. In the case of a conflict between any documents in this agreement that is not expressly resolved in those documents, their terms will control in the following order of descending priority: (1) this agreement, (2) the Product Terms, (3) the Online Services Terms, and (4) any other documents in this agreement.

l. **Survival.** All provisions survive termination of this agreement except those requiring performance only during the term of the agreement.

m. **U.S. export jurisdiction.** Products are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end-use and destination restrictions issued by U.S. and other governments related to Microsoft products, services, and technologies.

n. **Force majeure.** Neither party will be liable for any failure in performance due to causes beyond that party's reasonable control (such as fire, explosion, power blackout, earthquake, flood, severe storms, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism (including cyber terrorism), acts of God, acts or omissions of Internet traffic carriers, actions or omissions of regulatory or governmental bodies (including the passage of laws or regulations or other acts of government that impact the delivery of Online Services)). This Section will not, however, apply to your payment obligations under this agreement.

o. **Contracting authority.** If you are an individual accepting these terms on behalf of an entity, you represent that you have the legal authority to enter into this agreement on that entity's behalf.

10. Definitions.

Any reference in this agreement to "day" will be a calendar day.

"Acceptable Use Policy" is set forth in the Online Services Terms.

"Affiliate" means any legal entity that a party owns, that owns a party, or that is under common ownership with a party. "Ownership" means, for purposes of this definition, control of more than a 50% interest in an entity.

"Consumption Offering", "Commitment Offering", or "Limited Offering" describe categories of Subscription offers and are defined in Section 2.

"Customer Data" is defined in the Online Services Terms.

"End User" means any person you permit to access Customer Data hosted in the Online Services or otherwise use the Online Services.

"Fix" means a Product fix, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as Product service packs) or provides to Customer to address a specific issue.

"Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.

"Non-Microsoft Product" is defined in the Online Services Terms.

"Online Services" means any of the Microsoft-hosted online services subscribed to by Customer under this agreement, including Microsoft Dynamics Online Services, Office 365 Services, Microsoft Azure Services, or Microsoft Intune Online Services.

"Online Services Terms" means the additional terms that apply to Customer's use of Online Services published on the Licensing Site and updated from time to time.

"Previews" means preview, beta, or other pre-release version or feature of the Online Services or Software offered by Microsoft to obtain customer feedback.

"Product" means all products identified in the Product Terms, such as all Software, Online Services and other web-based services, including Previews.

"Product Terms" means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is published on the Licensing Site and is updated from time to time.

"Professional Services" means Product support services and Microsoft consulting services provided to Customer under this agreement. "Professional Services" does not include Online Services.

"Reseller" means an entity authorized by Microsoft to resell Software licenses and Online Service Subscriptions under this program and engaged by you to provide assistance with your Subscription.

"SLA" means Service Level Agreement, which specifies the minimum service level for the Online Services and is published on the Licensing Site.

"Software" means licensed copies of Microsoft software identified on the Product Terms. Software does not include Online Services, but Software may be a part of an Online Service.

"Subscription" means an enrollment for Online Services for a defined Term as established by your Reseller.

"Term" means the duration of a Subscription (e.g., 30 days or 12 months).

"Use Rights" means the use rights or terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. The Use Rights for Software are published by Microsoft in the Product Terms. The Use Rights for Online Services are published in the Online Services Terms.