STATE OF VERMONT PARTICIPATING ADDENDUM # 37983
FOR NASPO VALUEPOINT PURCHASING PROGRAM: CLOUD SOLUTIONS
Led by the State of Utah
Master Agreement #AR2489

Contractor: Smartronix, Inc.

Contractor's NASPO ValuePoint Webpage: https://www.naspovaluepoint.org/portfolios/portfolio-contractor/smartronix/

1. ***Parties.*** This Participating Addendum is a contract between the State of Vermont, through its Department of Buildings and General Services, Office of Purchasing & Contracting (hereinafter "State" or "Vermont"), and the Contractor identified above. It is the Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, the Contractor is required to have a Vermont Department of Taxes Business Account Number.

2. ***Subject Matter.*** This Participating Addendum authorizes the purchase of Cloud Solutions from Contractor pursuant to the Master Agreement identified above, which is hereby incorporated by reference. Contractor's awarded categories are:

    a. **Platform as a Service (PaaS)**: As used in the Participation Addendum 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.

    b. **Infrastructure as a Service (IaaS)**: As used in the Participation Addendum 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).

    c. **Software as a Service (SaaS)**: As used in this Participation Addendum 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.

3. ***Definitions.*** Capitalized terms used, but not defined herein, have the meanings ascribed to such terms in the Master Agreement between the Lead State and the Contractor.

4. ***Purchasing Entities.*** This Participating Addendum may be used by (a) all departments, offices, institutions, and other agencies of the State of Vermont and counties (each a "State Purchaser") according to the process for ordering and other restrictions applicable to State Purchasers set forth

herein; and (b) political subdivisions of the State of Vermont and any institution of higher education chartered in Vermont and accredited or holding a certificate of approval from the State Board of Education as authorized under 29 V.S.A. § 902 (each an "Additional Purchaser"). Issues concerning interpretation and eligibility for participation are solely within the authority of the State of Vermont Chief Procurement Officer. The State of Vermont and its officers and employees shall have no responsibility or liability for Additional Purchasers. Each Additional Purchaser is to make its own determination whether this Participating Addendum and the Master Agreement are consistent with its procurement policies and regulations.

5. ***Contract Term.*** The period of Contractor's performance shall begin on April 15, 2019 and end upon expiration of the Master Agreement, unless terminated earlier in accordance with the terms of this Participating Addendum or the Master Agreement. An amendment to this Participating Addendum shall not be necessary in the event of the renewal or extension of the Master Agreement.

6. ***Available Products and Services.*** All products, services and accessories listed on the Contractor's NASPO ValuePoint Webpage may be purchased under this Participating Addendum.

7. ***No Lease Agreements.*** Contractor is prohibited from leasing to State Purchasers under this Participating Addendum. Additional Purchasers are not subject to this prohibition and may negotiate lease agreements with Contractor if the terms of the Master Agreement permit leasing.

8. ***Requirements for Ordering.***

    a. Orders made under this Participating Addendum must include a specifically-negotiated Statement of Work or Service Level Agreement terms as necessary for the Product and/or Service to meet the Purchasing Entity's requirements. Orders funded by federal funds may include additional terms as necessary to comply with federal requirements.

        i. Prior to entering into Statement of Work or Service Level Agreement with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and/or Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

    b. State Purchasers must follow the ordering procedures of the State Contract Administrator to execute orders against this Participating Addendum, which shall include, as applicable, obtaining approval from the State CIO and/or Attorney General's Office prior to making purchases under this Participating Addendum.

    c. The State's Agency of Digital Services Procurement Office is the only entity authorized to place orders on behalf of State Purchasers. Contractor agrees that it will not accept or fulfill orders placed on behalf of State Purchasers from any other source. Contractor's failure to meet this requirement may result in suspension or termination of this Participating Addendum.

    d. All orders placed under this Participating Addendum must include the Participating Addendum Number on the Purchase Order.

9. ***Payment Provisions and Invoicing.***

a. Product offerings and complete details of product pricing, including discounts, applicable to this Participating Addendum are set forth in the Price Schedule maintained on-line at Contractor's NASPO ValuePoint Webpage listed above.

b. Purchasing Entities may solicit the Contractor or Fulfillment Partner/Authorized Reseller for deeper discounts than the minimum contract pricing as set forth in the Price Schedule (e.g., additional volume pricing, incremental discounts, firm fixed pricing or other incentives).

c. If applicable, all equipment pricing is to include F.O.B. delivery to the ordering facility. No request for extra delivery cost will be honored.

d. In the discretion of the Purchasing Entity, retainage may be specified in a Purchase Order, in an amount mutually agreeable to the parties.

e. Payment terms are Net 30 days from the date the State receives an error-free invoice with all necessary and complete supporting documentation. Invoices shall itemize all work performed during the invoice period, including, as applicable, the dates of service, rates of pay, hours of work performed, and any other information and/or documentation appropriate and sufficient to substantiate the amount invoiced for payment. As applicable, a copy of the notice(s) of acceptance shall accompany invoices submitted for payment.

f. Invoices shall be sent to the address identified on the Purchasing Entity's Purchase Order and shall specify the address to which payments will be sent. The State of Vermont Participating Addendum Number and Purchasing Entity's Purchase Order Number shall appear on each invoice for all purchases placed under this Participating Addendum.

g. Reimbursement of expenses is not authorized. All rates set forth in a Purchase Order shall be inclusive of any and all Contractor fees and expenses.

h. Unopened Products can be returned with no restocking fee up to 30 days from the date of receipt.

i. The State Purchasing Card may be used by State Purchasers for the payment of invoices. Use of the Purchasing Card requires all required documentation applicable to the purchase. The Purchasing Card is a payment mechanism, not a procurement approach and, therefore, does not relieve State Purchasers from adhering to all procurement laws, regulations, policies, procedures, and best practices.

10. ***Fulfillment Partners/Authorized Resellers.***

a. Resellers (or Fulfillment Partners) are available for this Participating Addendum if and to the extent approved by the State Chief Procurement Officer (each an "Authorized Reseller"). Any Authorized Resellers will be listed on the Contractor's NASPO ValuePoint Webpage listed above.

i. The State does not intend to approve resellers or fulfilment partners for this Participating Addendum except as required to provide services for certain Products (e.g., where a Product requires a managed service provider or other such services that Contractor is unable to provide without engaging a third party). Contractor shall notify the State when a Product requested by a Vermont Purchasing Entity will require

engagement of a third party. The State Chief Procurement Officer may, in its discretion, approve the third-party engagement on a limited basis, for the specific purchase only, or on a general basis, for whenever such Product is purchased under this Participating Addendum.

ii. A reseller or fulfilment partner approved by the State for this Participating Addendum is expressly not authorized to invoice State Purchasers directly. This provision shall not apply to Additional Purchasers.

b. All State policies, guidelines and requirements shall apply to Authorized Resellers.

c. Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions set forth by this Participating Addendum. Contractor acknowledges that each and all of the promises it makes as "Contractor" in the Master Agreement and in this Participating Addendum will apply to all Products and Services provided hereunder, regardless of who is providing or licensing the Product or performing the work.

i. Contractor promises that Purchasing Entities will not be required to affirmatively accept additional terms and conditions to use or access any Product or Service purchased under this Participating Addendum, whether by electronic means (e.g., click-through) or otherwise.

ii. Contractor promises that each of the third parties whose Products and/or Services are available for purchase under this Participating Addendum understand and agree that the terms and conditions applicable to their Products and/or Services are as set forth in the Master Agreement, as amended, and are subordinate to the terms of this Participating Addendum and the NASPO ValuePoint Master Agreement Terms & Conditions and associated service model Exhibits.

11. ***Reporting.*** Contractor shall submit quarterly reports electronically in the same format as set forth under the Master Agreement, detailing the purchasing of all items under this Participating Addendum. Contractor's reporting shall state "no activity" for any month in which there is no activity during a quarterly reporting period.

a. The reports shall be an excel spreadsheet transmitted electronically to SOV.ThePathForward@vermont.gov.

b. Reports are due for each quarter as follows:

Reporting Period	Report Due
January 1 to March 31	April 30
April 1 to June 30	July 31
July 1 to September 30	October 31
October 1 to December 31	January 31

c. Failure to meet these reporting requirements may result in suspension or termination of this Participating Addendum.

12. ***Prior Approvals.*** In accordance with current State law, bulletins, and interpretations, this Participating Addendum shall not be binding until it has been approved by the Vermont Attorney General's Office, the Secretary of Administration, and the State's Chief Information Officer.

13. ***Amendment.*** No changes, modifications, or amendments in the terms and conditions of this Participating Addendum shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.

14. ***Termination.*** This Participating Addendum may be terminated by the State at any time upon 30 days prior written notice to the Contractor. Upon termination or expiration of this Participating Addendum, each party will assist the other in orderly termination of the Participating Addendum and the transfer of all assets, tangible and intangible, as may facilitate the orderly, non-disrupted business continuation of each party. This provision shall not relieve the Contractor of the obligation to perform under any order executed prior to the effective date of termination or other expiration of this Participating Addendum.

15. ***Primary Contacts***. The Parties will keep and maintain current at all times a primary point of contact for this Participating Addendum. The primary contacts for this this Participating Addendum are as follows:

a. ***For the Contractor***:

Name:	Joel M. Parris
Phone:	317/485-5134
Email:	jmparris@smartronix.com

b. ***For the State***:

Name:	State of Vermont, Stephen Fazekas
Address:	109 State Street, Montpelier, VT 05633-3001
Phone:	802/828-2210
Fax:	802/828-2222
Email:	Stephen.fazekas@vermont.gov

16. Additional Terms and Conditions.

a. Notwithstanding any contrary language anywhere, in no event shall the terms of this contract or any document furnished by Contractor in connection with performance under this contract obligate the State to (1) defend or indemnify Contractor or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of Contractor or any third party.

b. If required by an order made by a State Purchaser under this Participating Addendum, the terms and conditions of the State of Vermont Business Associate Agreement, revised July 7, 2017 (the six-page document available online at: https://bgs.vermont.gov/sites/bgs/files/files/purchasing-

contracting/contracts/Attachment_E_BAA_HIPAA_071717REV.doc) shall be incorporated by reference and apply to the order. This provision shall not apply to Additional Purchasers.

c. Contractor is required at all times to comply with all applicable federal and state laws and regulations pertaining to information security and privacy.

d. **Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial:** This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Contractor in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. Contractor irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. Contractor agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Contractor agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.

e. **Sovereign Immunity:** The State reserves all immunities, defenses, rights or actions arising out of the State's sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State's immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State's entry into this Agreement.

f. **False Claims Act:** Contractor acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A. § 630 *et seq.* Contractor's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Contractor's liability.

g. **Whistleblower Protections:** Contractor shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, Contractor shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to Contractor or its agents prior to reporting to any governmental entity and/or the public.

h. **Fair Employment Practices and Americans with Disabilities Act:** Contractor agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Contractor shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by Contractor under this Agreement.

i. **Set Off:** The State may set off any sums which Contractor owes the State against any sums due Contractor under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures set forth in 32 V.S.A. § 3113.

j. **Taxes Due to the State**: Contractor certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, Contractor is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.

k. **Taxation of Purchases**: All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

l. **Certification Regarding Debarment**: Contractor certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Contractor nor Contractor's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds. Contractor further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Contractor is not presently debarred, suspended, nor named on the State's debarment list at: http://bgs.vermont.gov/purchasing/debarment

m. **Confidentiality**: Contractor acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

n. **Marketing**: Contractor shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

o. **Non-Appropriation**: If an order made under this Participating Addendum extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support the order, the State Purchaser may cancel the order at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. If the order is funded in whole or in part by Federal funds, and those Federal funds become unavailable or reduced, the State Purchaser may suspend or cancel the order immediately and shall have no obligation to pay from State revenues.

p. **Continuity of Performance**: In the event of a dispute between Contractor and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

q. **State Facilities**: If the State makes space available to Contractor in any State facility during the term of this Agreement for purposes of Contractor's performance under this Agreement, Contractor shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

r. **SOV Cybersecurity Standard 19-01**: All products and service provided to or for the use of the State under this Contract shall be in compliance with State of Vermont Cybersecurity Standard 19-01, which Contractor acknowledges has been provided to it, and is available on-

line at the following URL: https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives

By signing below Contractor agrees to offer the products and services on the Master Agreement at prices equal to or lower than the prices listed on the Master Agreement.

WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT

By the State of Vermont:

Date: _____

Signature: E-SIGNED by Christopher Cole on 2019-04-22 19:29:38 UTC

Name: Christopher Cole

Title: Commissioner
Buildings and General Services

By Smartronix, Inc.:

Date: 3/31/19

Signature: Melinda Armsworthy

Name: Melinda Armsworthy

Title: Director of Contracts

Contract # AR2489

STATE OF UTAH COOPERATIVE CONTRACT

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

Smartronix, Inc.		
Name		
44150 Smartronix Way		
Address		
Hollywood	MD	20636
City	State	Zip

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

Contact Person James Crowe Phone #703-435-3322 ext 102 Email jcrowe@smartronix.com
Vendor # VC205706 Commodity Code #920-05

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

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

4. CONTRACT PERIOD: Effective Date: 09/16/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.

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

6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including that attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
ATTACHMENT E: AWS Access Policy and Microsoft Cloud Solutions

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

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah State Procurement Code, Procurement Rules, and Contractor's response to Bid #CH16012.

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

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

CONTRACTOR

Melinda Armsworthy

Contractor's signature — Date: 8/26/16

Melinda Armsworthy, Contracts Lead
Type or Print Name and Title

STATE

for Director, Division of Purchasing — Date: 9.26.16

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

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. 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: The initial term of this Master Agreement is for ten (10) years with no renewal options.

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

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

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, 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.

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

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
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. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

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

[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.

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: 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 SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

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

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

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 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, 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 an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

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

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

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

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted

and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

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

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

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

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

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

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

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

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit 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 – Identification of Service Models Matrix

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

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Saas	Yes	Yes	Yes	private, public, community, and hybrid
IaaS	Yes	Yes	Yes	private, public, community, and hybrid
PaaS	Yes	Yes	Yes	private, public, community, and hybrid

Attachment C - Cost Schedule

[redacted]

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

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

Software as a Service **Discount %** 3%

Infrastructure as a Service **Discount %** 3%

Platform as a Services **Discount %** 3%

Value Added Services **Discount %** See attached

Additional Value Added Services:

Maintenance Services
Onsite Hourly Rate $ See attached
Remote Hourly Rate $ _____

Professional Services

- **Deployment Services**
  Onsite Hourly Rate $ See attached
  Remote Hourly Rate $ _____
- **Consulting/Advisory Services**
  Onsite Hourly Rate $ See attached
  Remote Hourly Rate $ _____
- **Architectural Design Services**
  Onsite Hourly Rate $ See attached
  Remote Hourly Rate $ _____
- **Statement of Work Services**
  Onsite Hourly Rate $ See attached
  Remote Hourly Rate $ _____

Partner Services
Onsite Hourly Rate $ See attached
Remote Hourly Rate $ _____

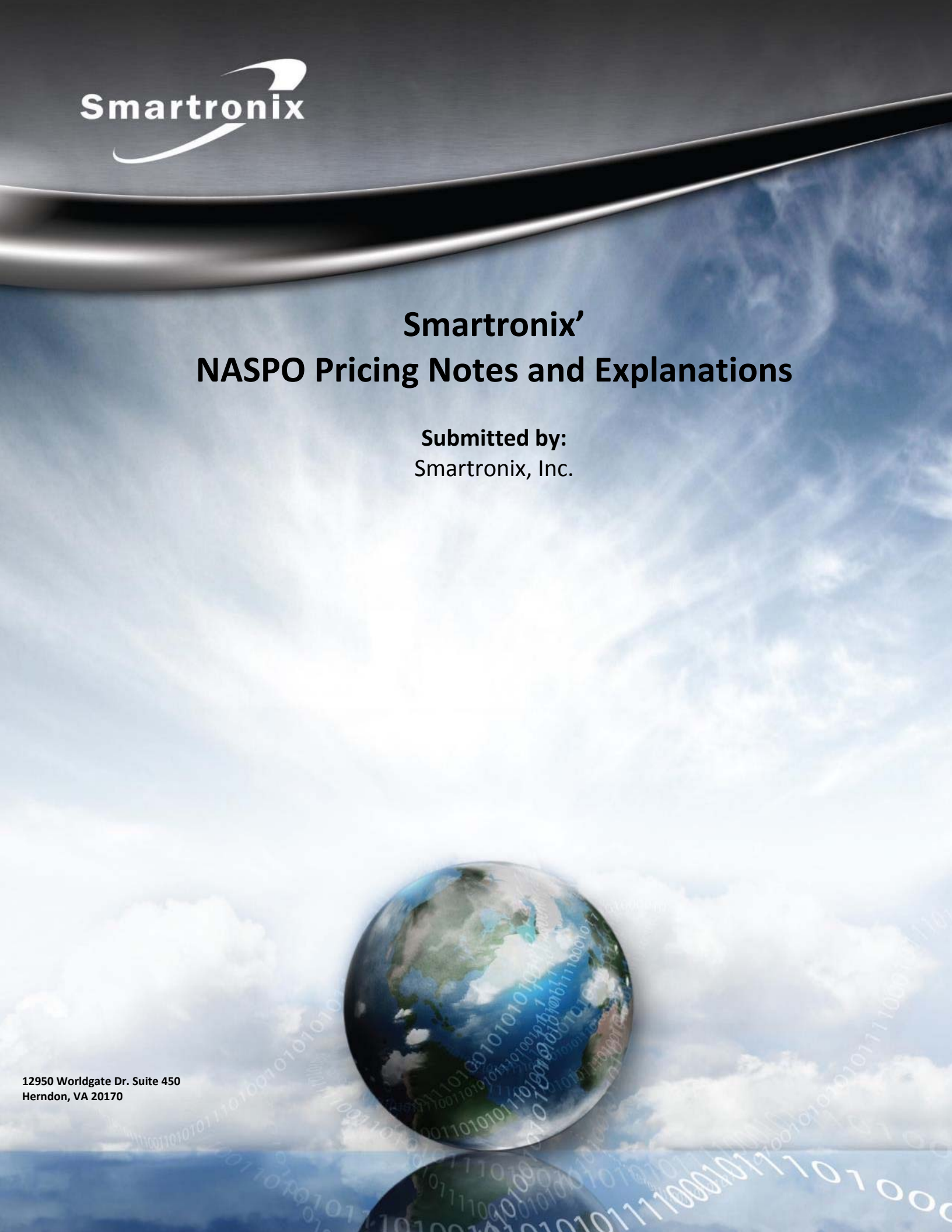
Training Deployment Services
Onsite Hourly Rate $ See attached
Online Hourly Rate $ _____

Smartronix'
NASPO Pricing Notes and Explanations

Submitted by:

Smartronix, Inc.

12950 Worldgate Dr. Suite 450
Herndon, VA 20170



1 NASPO PRICING NOTES AND EXPLANATIONS

Smartronix is pleased to provide the State of Utah with its pricing response to Bid #: CH16012. The attached NASPO Pricing offers pricing for the following Cloud Models: Iaas, Paas, SaaS. We are offering our Cloud Assured Managed Services (CAMS) for cloud services utilized in Public/Government Community Clouds.

The prices for Public and Government Community Cloud Services can be found within the same links provided in the price attachment and receive the same discounts, 3%. The pricing and discount schedule for Managed Services can also be found in the attached pricing.

Due to the rapid innovation and growth of available services in the cloud market place Smartronix is offering the use of all current and future cloud services as they are available. The current generation instance configurations can be found outlined in the attached pricing document. The full suite of products available to the state under contract with Smartronix can be found here:

- AWS: https://aws.amazon.com/products

Note: Not all services are available in all regions.
With current list pricing for all services can be found here:

- AWS: https://aws.amazon.com/pricing/services/

Pricing Methodology

Smartronix' approach to pricing and discounts based on consumption (or utility style), with Managed Service cost broken out from the cost of compute. We believe this model, of separating the cloud service and management costs provide the customer with the most flexible and transparency.

First we are offering discounts, outlined below, based on your month AWS spend. For example, utilizing CloudCheckr we run your AWS invoice at list price. We then discount that amount and invoice you. Our CAMS offering, invoiced separately, from your cloud services is priced per instance. In a variable environment where instances are stood up and shut down frequently we invoice the number of effective instances:

$$\frac{\text{Total hours consumed}}{\text{Total hours in that month}} = \text{\# of effective instances}$$

Cloud Services Price Estimating

AWS provide pricing calculators to estimate the cost of their services. These calculators are an important tool to estimate the cost of future task orders. And with all prices being publicly available there are no hidden cost. These calculators can be found here:

- AWS: http://calculator.s3.amazonaws.com/index.html

Discounting

We are offering the following discounts off of the list price at the time of consumption for each cloud provider:

- 3% on AWS cost

Note: There are no discounts provided on products and services sold thru Amazon AWS for which Smartronix does not receive a discount. This currently includes fees associated with: Amazon DevPay, Amazon Mechanical Turk, Amazon Flexible Payment Services and any 3rd party products purchased in the AWS Marketplace.

We are also offering a volume based discount off of the states's month managed service spend:

Monthly Cost	Vol Discount %
$0 - $15,000	0%
$15,000 - $30,000	2.5%
$30,000 - $45,000	5%
$45,000 - $60,000	10%
Over $60,000	12.5%

Additional services can be purchased utilizing our rate card:

Labor Category	Hourly Rate
Sr. Cloud Architect	$250
Cloud Architect	$225
Sr. Cloud Engineer	$200
Cloud Engineer	$180
Security Architect	$200
Security Analyst	$175
Sr. I&O Engineer	$140
I&O Engineer	$120
Cloud Program Manager	$220
Cloud Project Manager	$200

Amazon Web Services

Note 1: AWS pricing is based on per hour consumption.
Note 2: AWS Compute services vary between regional availability and OS
Note 3: When you have purchased a sufficient number of Reserved Instances in an AWS Region, you will automatically receive discounts on your upfront fees and hourly fees for future purchases of Reserved Instances in that AWS Region. Reserved Instance discounts are determined based on the total list price (non-discounted price) of upfront fees for the active Reserved Instances you have per AWS Region to determine the applicable volume discount tier. As an example, imagine that we had the following volume discount tiers:

- $0-$500K: Upfront - 0%, Hourly - 0%
- $500K - $4M: Upfront - 5%, Hourly - 5%
- $4M - $10M: Upfront - 10%, Hourly - 10%
- $10M+: Negotiated

PROFORMA IAAS/PAAS/SAAS COST TABLE

Vendor Name:	Smartronix, Inc			
				Comments
Period or Utilization Costs	**Description & Configuration Details**	**Unit Cost (Specify Units)**	**Vendors may submit their entire cost tables, BUT note that clarity and ease-of-use will be considered.**	
IaaS		SMX Pricing Response'		
PaaS		SMX Pricing Response'		
SaaS		SMX Pricing Response'		
Cloud Assured Managed Services (CAMS)				
Core Managed Services		$300.00	per instance/month	
Managed Services Light		$150.00	per instance/month	
Advanced Monitoring Services		$150.00	per instance/month	
Disaster Recovery Services		$175.00	per instance/month	
Enhanced Data Encryption Services		$200.00	per instance/month	
Advanced Security Services		$200.00	per instance/month - Requires Core Services	
Log Aggregation and Analysis		$1000 per month plus $5/GB daily indexed data	per environment/month	
Application Management Services		$300.00	per application instance/month	
Database Management Services		$500.00	per Database/month	
Web Management and CDN Services		$200.00	per property/month	
Infrastructure Advisory Support		$75.00	per instance Core Services Managed Instance/month	
Infrastructure Support Services		$2,900.00	per review/month - Requires Core Managed Services	
DevOps and CI/CD Services		$200.00	per instance/month	
FedRAMP Compliance and Continous Monitoring		$200.00	per instance/month - Requires Core Services and Advanced Security	
Notes:				
Discounting Schedule	Please see "SMX Discount Schedule" tab. Smartronix provides discounts for Support (CAMS), AWS and Azure. CAMS discounting is volume based off of the monthly dollar volume and AWS/Azure is a percentage discount off of the list price at the time of	SMX Discount Schedule		
AWS purchasing options	You can purchase AWS in 2 ways: On-Demand and Reserved Instances (RI). Ris can be purchased with no money up-front, partial up front payment and all up front payment. These 3 ways offer varying levels	https://aws.amazon.com/ec2/purchasing-options/		

Cloud Products and Services	Product Description	Product and Services Pricing
Smartronix:		
All Available Services thru AWS:	https://aws.amazon.com/products	https://aws.amazon.com/pricing/services/
Item	**Configuration (AWS)**	**Unit Cost (AWS)**
IaaS		
Managed Virtual Machines, Linux	See AWS Instance Config Tab	http://aws.amazon.com/ec2/pricing/
Managed Virtual Machines, Windows	See AWS Instance Config Tab	http://aws.amazon.com/ec2/pricing/
Storage	https://aws.amazon.com/ebs/	https://aws.amazon.com/ebs/pricing/
Virtual Private Cloud	https://aws.amazon.com/vpc/	https://aws.amazon.com/vpc/pricing/
Elastic Load Balancer	https://aws.amazon.com/elasticloadbalancing/	https://aws.amazon.com/elasticloadbalancing/pricing/
Dedicated Network Connection	https://aws.amazon.com/directconnect/	https://aws.amazon.com/directconnect/pricing/
DNS/LDAP servers *	https://aws.amazon.com/route53/	https://aws.amazon.com/route53/pricing/
Site to Site Connectivity	https://aws.amazon.com/directconnect/	https://aws.amazon.com/directconnect/pricing/
PaaS		
EMR	http://aws.amazon.com/elasticmapreduce/	http://aws.amazon.com/elasticmapreduce/pricing/
Relational Database Services	https://aws.amazon.com/rds/	https://aws.amazon.com/rds/pricing/
Elastic Container Services	https://aws.amazon.com/ecs/	https://aws.amazon.com/ecs/pricing/
Elastic BeanStalk	https://aws.amazon.com/elasticbeanstalk/	https://aws.amazon.com/elasticbeanstalk/pricing/
CodePipeline	https://aws.amazon.com/codepipeline/	https://aws.amazon.com/codepipeline/pricing/
OpsWorks	https://aws.amazon.com/opsworks/	https://aws.amazon.com/opsworks/pricing/
SaaS		
Amazon Simple Email Service	https://aws.amazon.com/ses/	https://aws.amazon.com/ses/pricing/
Amazon WorkSpaces	https://aws.amazon.com/workspaces/	https://aws.amazon.com/workspaces/pricing/
Amazon CloudSearch	http://aws.amazon.com/cloudsearch/	http://aws.amazon.com/cloudsearch/pricing/
Redshift	https://aws.amazon.com/redshift/	https://aws.amazon.com/redshift/pricing/

Note:
These services listed above are a sampling of they type of services per type that are available to the State of Utah.

Item	Discount	Comment
AWS Services	3%	Discount based off of current AWS list price at the time of consumption.

Smartronix Cloud Assured Managed Services (CAMS)

Monthly Cost	Vol Discount %
$0 - $15,000	0%
$15,000 - $30,000	2.5%
$30,000 - $45,000	5%
$45,000 - $60,000	10%
Over $60,000	12.5%

AWS Instance Types Matrix

Instance Type	vCPU	Memory (GiB)	Storage (GB)	Networking Performance	Physical Processor	Clock Speed (GHz)	Intel AVX†	Intel AVX2†	Intel Turbo	EBS OPT	Enhanced Networking†
t2.micro	1	1	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.small	1	2	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.medium	2	4	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.large	2	8	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.0	Yes	-	Yes	-	-
m4.large	2	8	EBS Only	Moderate	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.xlarge	4	16	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.2xlarge	8	32	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.4xlarge	16	64	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.10xlarge	40	160	EBS Only	10 Gigabit	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m3.medium	1	3.75	1 x 4 SSD	Moderate	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	-	-
m3.large	2	7.5	1 x 32 SSD	Moderate	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	-	-
m3.xlarge	4	15	2 x 40 SSD	High	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	Yes	-
m3.2xlarge	8	30	2 x 80 SSD	High	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	Yes	-
c4.large	2	3.75	EBS Only	Moderate	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.xlarge	4	7.5	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.2xlarge	8	15	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.4xlarge	16	30	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.8xlarge	36	60	EBS Only	10 Gigabit	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c3.large	2	3.75	2 x 16 SSD	Moderate	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	-	Yes
c3.xlarge	4	7.5	2 x 40 SSD	Moderate	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.2xlarge	8	15	2 x 80 SSD	High	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.4xlarge	16	30	2 x 160 SSD	High	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.8xlarge	32	60	2 x 320 SSD	10 Gigabit	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	-	Yes
g2.2xlarge	8	15	1 x 60 SSD	High	Intel Xeon E5-2670	2.6	Yes	-	Yes	Yes	-
g2.8xlarge	32	60	2 x 120 SSD	10 Gigabit	Intel Xeon E5-2670	2.6	Yes	-	Yes	-	-
r3.large	2	15.25	1 x 32 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes
r3.xlarge	4	30.5	1 x 80 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.2xlarge	8	61	1 x 160 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.4xlarge	16	122	1 x 320 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.8xlarge	32	244	2 x 320 SSD	10 Gigabit	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes
i2.xlarge	4	30.5	1 x 800 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.2xlarge	8	61	2 x 800 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.4xlarge	16	122	4 x 800 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.8xlarge	32	244	8 x 800 SSD	10 Gigabit	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes
d2.xlarge	4	30.5	3 x 2000	Moderate	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.2xlarge	8	61	6 x 2000	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.4xlarge	16	122	12 x 2000	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.8xlarge	36	244	24 x 2000	10 Gigabit	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes

Notes:
Each vCPU is a hyperthread of an Intel Xeon core for M4, M3, C4, C3, R3, HS1, G2, I2, and D2.
*M3 instances may also launch as an Intel Xeon E5-2670 (Sandy Bridge) Processor running at 2.6 GHz.
† AVX, AVX2, and Enhanced Networking are only available on instances launched with HVM AMIs.
Looking for T1, M1, C1, CC2, M2, CR1, CG1, HS1, or HI1 Instances? See the Previous Generation Instances page.

Core Managed Services	
Service Title	**Description**
Monitoring and Notification	Systems, services and cloud components monitoring which provides real time view of your entire cloud environment. Performance, usage and availability for customer specific components are monitored. Monitoring can be configured to provide specific notifications based on availability and captured events within the environment.
IT Service Management	CloudAssured Support is provided 24x7x365 through email, phone support, and the web. Ticket status change notifications are provided back to customers automatically. Customers have access to tickets and status reports for incidents and problems through the CloudAssured Portal.
SLA Management	On Demand view of Smartronix' performance against SLAs in the CloudAssured Portal.
CloudAssured Portal	The CloudAssured portal provides a consolidated view of monitoring and notification information, , ticket status, and billing information provided by Smartronix Managed Services. Access to your portal is role-based to limit user access.
Incident Response	This service provides analysis, tracking, and corrective actions for issues impacting customer environments and infrastructure. As well as limits damage and reduces recovery time and costs associated with an unplanned event.
Antivirus (AV) Management	Antivirus management provides protection against malware for the customer environment by ensuring that the AV software is installed, maintained, up to date and running current malware signatures. When malware is detected we proactively ensure quarantine and an incident ticket is automatically created for the remediation of the issue. Audits are performed to ensure individual server compliance.
Boundary Management	A proactive monitoring and management service that provides configuration of cloud service provider components for networking, firewall, VPN, subnets, ACL and virtual networks.
Log Aggregation	The Log Aggregation is utilized to capture IaaS native Logs e.g Cloud Trail and System, application and firewall logs to object files for troubleshooting and analysis. Alerts are generated for critical events and key performance indicators within the environment to trigger operational response.
Patch Management for OS	Monitoring and applying operating system patches and updates through the use of a patch management life-cycle, which includes the complete assessment and testing of patches prior to applying them.
Backup Services	Backup Services provide for system, environment and cloud services backup and restore. Backups are stored within the customer cloud environment and all data costs associated with backups are part of the customer cloud environment costs.
Billing	Customers are provided a consolidated bill of all provided services. For customers where we are providing resale of cloud services, a single consolidated bill showing all cloud charges and managed services is provided based on monthly usage. Additionally the level of billing detail is flexible and may be designed to support customer requirements and may be used for chargeback purposes.
Billing Advisory Services	Smartronix proactively reviews and provides customers with recommendations on optimization of cloud environments for lowering your cloud costs and improving performance based on our knowledge of the environment and utilization levels. Cloud usage is also included to provide insight into underutilized or unused components within the environment.
Managed Services Light	

Service Title	Description
Monitoring and Notification	Systems, services and cloud components monitoring which provides real time view of your entire cloud environment. Performance, usage and availability for all customer specific components are monitored. Monitoring can be configured to provide specific notifications based on availability and captured events within the environment. Cloud usage is also included to provide insight into underutilized or unused components within the environment.
Ticketing	CloudAssured Support is provided 24x7x365 through email, phone support, and the web. Ticket status change notifications are provided back to customers automatically. Customers have access to tickets and status reports for incidents and problems through the CloudAssured Portal.
SLA Management	On Demand view of Smartronix' performance against SLAs in the CloudAssured Portal.
CloudAssured Portal	The CloudAssured portal provides a consolidated view of monitoring and notification information, SLAs, ticket status, billing information and security information provided by Smartronix Managed Services. Access to your portal is role-based to limit user access based on need and risk.
Incident Response	This service provides analysis, tracking, and corrective actions for issues impacting customer environments and infrastructure. As well as limits damage and reduces recovery time and costs associated with an unplanned event.
Antivirus (AV) Management	Antivirus management provides protection against malware for the customer environment by ensuring that the AV software is installed, maintained, up to date and running current malware signatures. When malware is detected we proactively ensure quarantine and an incident ticket is automatically created for the remediation of the issue. Audits are performed to ensure individual server compliance.
Boundary Management	A proactive monitoring and management service that provides configuration of cloud service provider components for networking, firewall, VPN, subnets, ACL and virtual networks.
Billing	Customers are provided a consolidated bill of all provided services. For customers where we are providing resale of cloud services, a single consolidated bill showing all cloud charges and managed services is provided based on monthly usage. Additionally the level of billing detail is flexible and may be designed to support customer requirements and may be used for chargeback purposes.
Billing Advisory Services	Smartronix proactively reviews and provides customers with recommendations on optimization of cloud environments for lowering your cloud costs and improving performance based on our knowledge of the environment and utilization levels.

Optional Services	
Service Title	**Description**
Log Aggregation and Analysis	The Log Aggregation and Analysis service is utilized to capture all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.
Infrastructure Advisory Services	Smartronix proactively reviews and provides customers with recommendations on optimization of cloud services to include capacity management reviews, architectural reviews and best practices, auto scaling approaches, and design services.

Disaster Recovery Services	Disaster recovery services provide full planning, annual testing and execution of a disaster recovery solution which encompasses customer applications, systems, and environments to provide continuity of service.
Advanced Monitoring Services/ Perfo	Application, transactional, synthetic and additional performance management and monitoring services may be configured for customer applications, systems and environments.
Enhanced Data Encryption Services	Examples of Enhanced Data Encryption Services include: 1. Use of hardware security modules 2. Database and/or Application Level 3. Key management and key rotation services
Advanced Security Services	Customer specific advanced security services including data loss prevention, advanced identity management services, host based IPS, security assessments, continuous security monitoring and additional services are available to create high security enclaves within cloud environments.
Application Management Services	Full lifecycle application management is available for COTS and custom built applications. This includes monitoring, maintenance, patching and security assessments for these applications. This service can also provide the customer with application specific availability or performance service level agreements. Application specific backup services may also be provided upon request. (Limited to minor patches of supported COTS products, not major version upgrades) and configuration management of changes to the environment.
Database Management Services	Full lifecycle database management is available for industry leading database vendors. This includes monitoring, maintenance, patching and security assessments for these databases. This service can also provide the customer with database specific availability or performance service level agreements. Database specific backup services may also be provided upon request.
Web Management Services and CDN	This service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks. This includes the operations and management of third party CDN services as well. We will provide proactive security monitoring of the site distribution, availability monitoring, including optionally available outside availability and performance monitoring, patching of the environment and applications (limited to minor patches of supported COTS products, not major version upgrades) and configuration management of changes to the site distribution. For CDN services this will include configuration, monitoring, availability and maintenance of the CDN services.
DevOps and CI/CD Services	A pre-configured environment, customized to customer needs, which allows for continuous integration, continuous deployment and full lifecycle DevOps is available and provided as a fully managed service to customers. This includes the use of orchestration tools, code repositories, testing suites, workflow management, service deployment, and automated scaling of environments.

Smartronix

Technical Quote
STATE OF UTAH
Cloud Services
CH16012

March 10th, 2016

Submitted by:

Smartronix, Inc.

TABLE OF CONTENTS

1. RFP SIGNATURE PAGE

Smartronix submitted the RFP signature page via the BidSync website.

2. EXECUTIVE SUMMARY

Smartronix is providing the entire catalog of Amazon Web Services cloud services combined with our FedRAMP 3PAO authorized Cloud Assured Managed Services™ capabilities. This combined offering enables all of the NASPO Participating Entities to choose from a wide array of cloud solution offerings that will positively transform the way IT services are delivered and consumed. Throughout this proposal we will demonstrate our unique expertise and long history of delivering AWS cloud services including solutions we have built for the US Department of the Treasury, IRS, Department of the Interior, Department of Defense, Health and Human Services, Veterans Administration, Federal Reserve Bank and a wide range of Fortune 1000 enterprises including Dole Foods, Discover Financial, the National Football League, and Fannie Mae, to name a few.

No other AWS partner has the depth of experience in deploying AWS services into heavily regulated and security compliance driven domains. We were the first AWS Partner to bring cloud services to the government starting back in 2009 with Recovery.gov and in 2010 with Treasury.gov and dozens of other high profile Treasury web properties. Over the past 7 years of working closely with AWS we have developed the largest cadre of government-cleared resources trained on the AWS platform and we look forward to bringing this expertise to NASPO.

Our complete service catalog includes IT Transformation Strategy, Cloud Assessment and Application Rationalization, Cloud Optimized Design and Migration, Security Management, and 24x7x365 Managed Service Provider capabilities. Our solutions have been specifically tailored to designing, managing, and operating government workloads and maintaining strict security and compliance standards. We have elected to provide AWS IaaS, PaaS, and SaaS service models covering each deployment model (private, public, community, and hybrid.) and at all FIPS 199 data classification levels (Low Impact through High). We are confident in our unique ability to secure, manage, and protect government assets and workloads in the cloud.

Why Smartronix and AWS for NASPO?

Reason 1: AWS Breadth of Service Offerings

Figure 1: Entire AWS Service Catalog including Infrastructure, Platform, and Software Services

Figure 2: Gartner Magic Quadrant for IaaS – 2015

AWS has the most advanced set of cloud services available on the market and their pace of innovation has been staggering. Gartner's profile of AWS has them as the leading vendor in both completeness of vision and ability to execute. "It is the overwhelming market share leader, with over 10 times more cloud IaaS compute capacity in use than the aggregate total of the other 14 providers in this Magic Quadrant." Gartner also states: "AWS is a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market. It has the richest array of IaaS features and PaaS-like capabilities. It continues to rapidly expand its service offerings and offer higher-level solutions."

Adoption of AWS cloud services will be highly transformative for NASPO's Participating Entities. With the right consulting partner AWS services can be deployed securely, reliably, and highly cost effective.

Reason 2: Smartronix AWS Partnership and Experience

Smartronix developed its expertise in IT enterprise infrastructure management with the development, design, implementation and operation of large scale geographically dispersed networks and enterprise class application development services. We were early adopters of virtualization technologies and have continued our investment in the development of our people, processes and technology within our cloud practice. **We are currently an Amazon Web Services (AWS) Premier Partner for an unprecedented 4 straight years which places us in the .1% of the more than 10,000 AWS partners globally.**

Figure 3: AWS Partner Network

Further, our pioneering efforts in providing technically superior cloud solutions for highly regulated federal customers have been recognized by AWS with the distinction of being one of the select few Authorized Government Partners. We have been designated as an official AWS Managed Service Provider and our Cloud Assured™ Services allow our customers to leverage the power and scalability of AWS while reducing the cost and complexity of managing and monitoring cloud infrastructure and applications in-house. We recently completed an AWS-sponsored audit of our managed services and were the only company that scored 100%.

Agencies that are heavily invested in building cloud based assets recognize the critical value of working with an experienced cloud services vendor that is able to deliver expertise and knowledge of transition, architecture, and operational support of these technologies. Smartronix provides the full lifecycle of cloud computing services--from concept, strategy, assessment, and secure designs through deployment, migration, optimization, and continued operations support.

Among AWS Premier Partners, Smartronix stands out for its deep technical expertise and its ability to design and develop the right solution for clients in regulated industries—Government, Healthcare, and Financial — where security and compliance are paramount. Our background in Virtualization, Network Operations, and Cyber Security allowed us to lead the way for AWS and introduce them into the Federal government with Recovery.gov in 2009 and with the development of the first FISMA Moderate Platform for the United States Department of the Treasury in 2010. Additionally, Smartronix understands the intricacies of deploying solutions on AWS GovCloud and was one of the first companies to deploy capabilities in that region. We also deployed the first cabinet level FedRAMP Compliant cloud service for the Treasury in 2014.

Smartronix currently has nearly 700 employees, of which over 70% are cleared. We have a large number (100+) of certified Security Experts with a variety of qualifications including CISSP, Certified Ethical Hackers, CISM, CCNA Security, GSEC, and other security certifications. Additionally, we currently have over 150 people certified and/or accredited on AWS and are one of Amazon Web Service's largest Channel Resellers. We are original members of the group of Authorized Government Partners and Authorized Government Resellers. Due to our volume of resale we can also offer discounts substantially larger than our competitors.

Reason 3: Highly acclaimed 24x7x365 Managed Services Provider

Gartner recently profiled the leading AWS Managed Services Providers and distinguished Smartronix as "*a* Hybrid MSP offering a variety of services, not all of which are directly cloud-related. They have a significant AWS-related managed and professional services practice."

Gartner went on to state that the MSPs they profiled all have a "... proven success delivering services on the AWS platform" further clarifying that: "Smartronix works with midmarket, enterprise and government customers. It can serve either Mode 1-oriented or Mode 2-oriented customers, although it is more likely to work with Mode 1 customers that are trying to gain some agility or reduce costs by moving to the cloud. Smartronix targets customers in heavily regulated industries, and those that must meet stringent security requirements in the cloud."

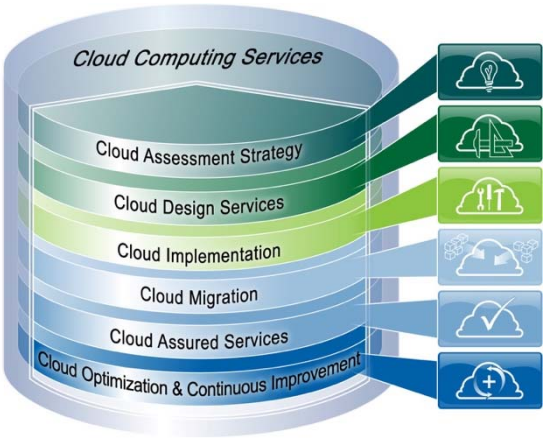


Figure 4: Smartronix Services Stack

Hybrid MSPs are exactly what NASPO Participating Entities require. Our knowledge of existing on-premises infrastructure coupled with our vast experience in extending, migrating, optimizing, and securely managing deployments in the cloud will help NASPO customers increase their technical efficiency, reduce costs, drive cost transparency, improve scalability and availability of services, enhance security, and modernize their approach to service delivery. We have helped more government customers in their transformation to the cloud than any other partner. We provide all of the ancillary services surrounding AWS that NASPO customers will require.

Our size, our company locations, our past performance, our understanding of legacy infrastructure, our longstanding partnership with AWS, and our commitment to helping our customers receive value in deploying and consuming cloud based services makes us an ideal partner to meet the wide variety of needs of your constituents. We respectfully look forward to the opportunity to provide the highest quality of cloud service solutions.

3. MANDATORY MINIMUMS

3.1. COVER LETTER (RFP 5.2)

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

Smartronix submitted a signed Cover Letter via the BidSync website.

3.1. ACKNOWLEDGEMENT OF AMENDMENTS (RFP 5.3)

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

Smartronix submitted an Acknowledgement of Amendments to RFP 02102016 via the BidSync website.

3.2. EXECUTIVE SUMMARY (RFP 5.4)

Included in Section 2

3.3. GENERAL REQUIREMENTS (RFP 5.5)

3.3.1. Usage Report Agreement (RFP 5.5.1)

Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Smartronix agrees to the condition that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

3.3.2. Cooperation Statement (RFP 5.5.2)

Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Smartronix agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

3.3.3. CSA STAR self-assessment (RFP 5.5.3)

Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment2. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

AWS is compliant with Level 1 CSA STAR Registry Self-Assessment. Please refer to AWS' self-assessment found within our Risk and Compliance Whitepaper, which is included as Attachment I to this proposal.

This is the latest CAIQ (v3) released by the CSA.

Per the CSA definitions, AWS aligns with Level 2 via the determinations in our third party audits for SOC and ISO:

Level 2 Attestation is based on SOC2, which can be requested under NDA - http://aws.amazon.com/compliance/contact/ The SOC 2 report audit attests that AWS has been validated by a third party auditor to confirm that AWS' control objectives are appropriately designed and operating effectively.

Level 2 Certification is based on ISO 27001:2005 – the AWS ISO 27001:2005 certification is available on our website: http://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

All of the AWS self-assessed assertions within the CSA STAR Registry Self-Assessment are backed by independent, third party audits across multiple compliance programs. We continue to assert we raise the bar on CSA's "attestation" and "certification" program.

Consensus Assessments Initiative Questionnaire (CAIQ)

AWS has completed CSA Consensus Assessments Initiative Questionnaire with answers provided on pages 25-61 of Amazon Web Services Risk and Compliance Whitepaper, included as Attachment I to this proposal.

3.3.4. SLAs (RFP 5.5.4)

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

Smartronix SLA's
Smartronix will pass through in its entirety the AWS SLAs for uptime, durability, and availability of services. This includes the financially backed penalties associated with missing SLAs.

AWS currently provides Service Level Agreements (SLAs) for several products. Due to the rapidly evolving nature of AWS's product offerings, SLAs are best reviewed directly on their website via the links below:

- Amazon EC2 SLA: http://aws.amazon.com/ec2-sla/
- Amazon S3 SLA: http://aws.amazon.com/s3-sla
- Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/

- Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/
- Amazon RDS SLA: http://aws.amazon.com/rds-sla/

Highlights of the SLAs are listed below.

Service Commitments and Service Credits
Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for either Amazon EC2 or Amazon EBS (whichever was Unavailable, or both if both were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	30%

By providing a solution built on AWS using EC2, multiple availability zones, elastic load balancing and auto-scaling the solutions will be able to provide an uptime that meets or exceeds 99.99%. EC2 currently provides an SLA backed uptime of 99.95% to customers. Utilizing two separate data centers (availability zones) within the same region will eliminate a single data center issue causing operational impact. Through the utilization of elastic load balancing and auto-scaling the systems, customers will be able to utilize multiple redundant servers to service users. This approach also mitigates system downtime issues allowing you to exceed the AWS SLA of 99.95% availability.

Backup Capability
AWS provides the ability to do daily incremental and weekly full snapshot capabilities. Backups are stored in S3, which provides multi-zone redundancy and eleven 9's of durability. (99.999999999%)

Backup retention periods can be set by policy to determine the length of time snapshots are kept or moved through the storage lifecycle into cold storage (archives).

Scalable Resources
AWS enables the ability increase/decrease resources to support unpredictable high/low usage. Several available CloudWatch metrics or custom metrics can trigger elasticity for servers and database instances. Autoscaling configurations support the ability to scale out servers under load balancers to support increased utilization requirement for compute and bandwidth. S3 provides nearly unlimited storage elasticity. Container services enable automated elasticity for software services.

Support
As Smartronix is providing Resale services, we will also provide first tier support to access the Smartronix Business Support services. These services are inclusive of AWS Business Support services plus our 24x7x365 quick response portal. Smartronix will enable customers to have direct support requests to AWS as well as proxying requests through our 24x7 help desk.

Monitoring

Smartronix will provide customers with complete access to AWS capabilities for monitoring their cloud services for utilization, performance, and status including the ability to add custom metrics through CloudWatch.

Systems Monitoring and Support

Smartronix will provide direct access to AWS support for 24x7x365 support for all infrastructure outages and SLA failures. Smartronix will provide troubleshooting services and support during core duty hours for all infrastructure hosting related services. Where required Smartronix will ensure AWS specific related issues are seamlessly relayed to AWS Business Support for prompt resolution.

Support Requests

Smartronix provides 24x7x365 access to our CloudAssured Managed Services team. This team provides tier 3 support to address AWS infrastructure related issues. This team works closely with AWS Business Support and will escalate to AWS when necessary. Alternatively, customers will have direct access to AWS Business Support as well via email, phone, or web support through their case management system. Smartronix provides support via phone and our ServiceNow incident management portal.

3.4. RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS (RFP 5.7)

Smartronix acknowledges that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

4. BUSINESS PROFILE (RFP 6)

4.1. BUSINESS PROFILE (RFP 6.1)

4.1.1. About Smartronix

Smartronix, founded in 1995 and headquartered in Hollywood, MD is a global professional solutions provider specializing in Cloud Computing, Enterprise Software Solutions, Network Operations, Cyber Security and Health IT solutions serving an equal mix of commercial and government customers across the US. Smartronix has been leading the cloud computing movement since 2009, with unparalleled expertise in building secure cloud-based solutions with a proven delivery model. Smartronix developed its expertise in IT enterprise infrastructure management with the development, design, implementation and operation of large scale geographically dispersed networks and enterprise class application development services. We were early adopters of virtualization technologies and have continued our investment in the development of our people, processes and technology within our cloud practice. **We are currently an Amazon Web Services (AWS) Premier Partner for an unprecedented 4 straight years which places us in the top .1% of all AWS partners globally.**

Figure 5: AWS Partner Network

Smartronix has unique expertise and a long history of delivering AWS cloud services including solutions we have built for the US Department of the Treasury, IRS, Department of the Interior, Department of Defense, Health and Human Services, Veterans Administration, Federal Reserve Bank and a wide range of Fortune 1000 enterprises including Dole Foods, Discover Financial, the National Football League, Fannie Mae, and Panasonic to name a few. No other AWS partner has the depth of experience in deploying AWS services into heavily regulated and security compliance driven domains. We were the first AWS Partner to bring cloud services to the government starting back in 2009 with Recovery.gov and in 2010 with Treasury.gov and dozens of other high profile Treasury web properties. Over the past 7 years of working closely with AWS we have developed the largest cadre of government cleared resources trained on the AWS platform.

Further, our pioneering efforts in providing technically superior cloud solutions for highly regulated federal customers have been recognized by AWS with the distinction of being one of the select few Authorized Government Partners. We have been designated as an official AWS Managed Service Provider and our Cloud Assured™ Services allow our customers to leverage the power and scalability of AWS while reducing the cost and complexity of managing and monitoring cloud infrastructure and applications in-house. We recently completed an AWS-sponsored audit of our managed services and were the only company that scored 100%.

Among AWS Premier Partners, Smartronix stands out for its deep technical expertise and its ability to design and develop the right solution for clients in regulated industries—Government, Healthcare, and Financial — where security and compliance are paramount. Our background in Virtualization, Network Operations, and Cyber Security allowed us to lead the way for AWS and introduce them into the Federal government with Recovery.gov in 2009 and with the development of the first FISMA Moderate Platform for the United States Department of the Treasury in 2010. Additionally, Smartronix understands the intricacies of deploying solutions on AWS GovCloud and was one of the first companies to deploy capabilities in that region. We also deployed the first cabinet level FedRAMP Compliant cloud service for the Treasury in 2014.

Smartronix currently has nearly 700 employees, of which over 70% are cleared. We have a large number (100+) of certified Security Experts with a variety of qualifications including CISSP, Certified Ethical Hackers, CISM, CCNA Security, GSEC, and other security certifications. Additionally, we currently have over 150 people certified and/or accredited on AWS.

Our dedicated cloud practice has year over year growth of over 75% in the past 4 years with our cloud revenue nearly doubling last year alone. The Cloud Services team has grown to over 150 individuals with a 93% retention rate.

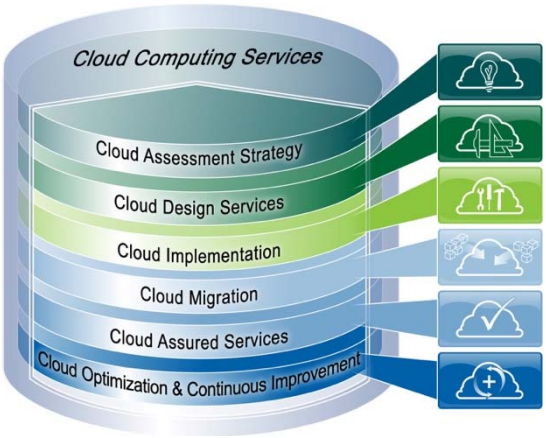


Figure 6: Smartronix Services Stack

Gartner recently profiled the leading AWS Managed Services Providers and distinguished Smartronix as *"a* Hybrid MSP offering a variety of services, not all of which are directly cloud-related. They have a significant AWS-related managed and professional services practice."

Gartner went on to state that the MSPs they profiled all have a "... proven success delivering services on the AWS platform" further clarifying that: "Smartronix works with midmarket, enterprise and government customers. It can serve either Mode 1-oriented or Mode 2-oriented customers, although it is more likely to work with Mode 1 customers that are trying to gain some agility or reduce costs by moving to the cloud. Smartronix targets customers in heavily regulated industries, and those that must meet stringent security requirements in the cloud."

Smartronix is a trusted solution provider of AWS and have a strong track record of delivering value and customer satisfaction to our joint customers. We look forward to working with Smartronix as they bring the benefits of cloud computing to government customers.

Sincerely,

Teresa Carlson
Vice President, Global Public Sector

Amazon Web Services, 13461 Sunrise Valley Drive Herndon, Virginia 20171

Figure 7 - Excerpt of Letter of Recommendation from AWS Global Public Sector, VP

We have been recognized by the AWS Global Public Sector leadership for providing exceptional technical support services to our clients and expanding the deployment of solutions on AWS EC2, as seen in **Figure 7** above.

AWS Overview

Amazon has a long history of using a decentralized IT infrastructure. This has enabled our development teams to access compute and storage resources on demand, and it has increased overall productivity and agility. By 2005, Amazon had spent over a decade and millions of dollars building and managing the large-scale, reliable, and efficient IT infrastructure that powered one of the world's largest online retail platforms. Amazon launched Amazon Web Services, Inc. (AWS) so that other organizations could benefit from Amazon's experience and investment in running a large-scale, distributed, transactional IT infrastructure. AWS has been operating since 2006 and now serves more than one million active customers worldwide.

Using AWS, customers can requisition compute power, storage, and other services in minutes and have the flexibility to choose the development platform or programming model that makes the most sense for the problems they are trying to solve. Customers pay only for what they use, with no up-front expenses or long-term commitments, making AWS a cost-effective way to deliver applications.

The Differences that Distinguish AWS

AWS is readily distinguished from other vendors in the traditional IT computing landscape because it is:

- **Flexible.** AWS enables organizations to use the programming models, operating systems, databases, and architectures with which they are already familiar. In addition, this flexibility helps organizations mix and match architectures in order to serve their diverse business needs.
- **Cost effective.** With AWS, organizations pay only for what they use, without up-front costs or long-term commitments.
- **Scalable and elastic.** Organizations can quickly add and subtract AWS resources to and from their applications in order to meet customer demand and manage costs.
- **Innovative.** AWS launched 722 new services and features in 2015. Our pace of innovation is funded and sustained through our economies of scale and commitment to delivering the products and services that matter most to our customers. Our continual innovation ensures that customers maintain state-of-the-art IT infrastructure without having to make recapitalization investments.
- **Secure.** In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides the appropriate security features in those services, and documents how to use those features.
- **Experienced**. When using AWS, organizations can leverage AWS's many years of experience delivering large-scale, global infrastructure in a reliable, secure fashion.

4.2. SCOPE OF EXPERIENCE (RFP 6.2)

Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred.

Smartronix' experience in reselling and supporting AWS services to Federal customers is unparalleled, we have been providing AWS cloud infrastructure to the Federal government since 2009. Smartronix currently provide consulting, managed services, cloud resale and additional services for over one hundred Commercial, Government and DoD customers operating on the AWS environment. Our clients include the US Department of the Treasury, Department of Interior, Consumer Financial Protection Bureau, Department of Labor, Recovery Accountability and Transparency Board, Internal Revenue Service, and the Naval Space and Warfare Command. Smartronix provides a cost-effective and responsive solution to acquire FedRAMP Hosting Solutions. With Smartronix, you are partnering with a firm with a proven track record in the delivery of cloud-based solutions that brings:

- An experienced and mature delivery organization that has successfully delivered FedRAMP Hosting Solutions to US Federal, DOD and Commercial clients since 2009;
- Highly qualified and AWS certified staff with real-world implementation expertise of FedRAMP, FISMA/DIACAP C&A'd systems;
- Deep corporate and technical relationship as an AWS Authorized Government Reseller, and Premier Consulting Partner
- Financially stable service provider with fulfillment capabilities including program management, procurement support, financial management and business support

Certified delivery processes with ISO 9001, CMMI Level 3 and ISO 20000 certifications.

No other provider has the breadth and depth of expertise in delivering highly available and highly scalable cloud solutions. As a CMMI Level 3, ISO 9001 and ISO 20000 certified organization, we use ITIL best practices as the framework for our service delivery processes. Our ISO/IEC 20000-2011 scope includes all of our Managed Cloud Hosting and Services Offerings. We possess one of the largest and most talented collections of trained and certified Solution Architects on the Amazon Web Services (AWS) platform.

Past Performance Citations

SPAWAR Systems Center Atlantic AWS Services and Support

1. **Contract Number:** HHSN316201200047W Order # N65236-12-D-047W
2. **Description and Relevance:** Smartronix provides SPAWAR's Cloud Services Integration (CSI) IPT a cost-effective and responsive solution to acquire Amazon Web Services (AWS) Cloud Computing services, a geographically Dispersed Hosting and Networking Services. By providing SPAWAR with the capability to use load balancing to automatically distribute incoming application traffic across multiple instances and enable greater fault tolerance as well as offer distribution functionality to make downloading and uploading items quicker for SPAWAR LANT. We work as an active member of the CSI IPT ensuring the rapid fulfillment of Cloud Hosting Service needs. We ensure the

fulfillment of requests via accredited AWS in Amazon's GovCloud, East, and West Regions and provide business & technical support including training necessary to ensure CSI IPT's ability to provision, monitor and manage AWS Cloud Computing Services.
Smartronix also provides authorized SPAWAR administrators with access to a web based Management Console that unifies and simplifies the user experience across these different areas of functionality. The user experience begins with a secure login for authentication, and then their resources access can be managed in the Identity and Access Management (IAM) service. All elements of the Console are user-targeted based on their specific needs. As such, all users must be authenticated to access the portal. Once in the portal, users only see the elements for which they have permissions.
Smartronix provides utility-based Computing Services for Amazon Web Services. By providing AWS services in a utility model DON is only billed for services that are reserved for, or consumed by, them, during the prior billing period. DON will have nearly unlimited resources available to them and will be responsible for their resource consumption and commitment of reservation of resources.
The SPAWAR AWS Services and Support contract is valued at approximately $8.4M

3. **Period of Performance:** 11/1/2013 – Ongoing

Treasury BPA

1. **Contract Number:** GS-35F-0362J, Order#: TIRNO-13-Z-00007
2. **Description and Relevance:** Smartronix engineers architected, deployed and maintained a FedRAMP Moderate managed Amazon Cloud platform called Workplace.gov Community Cloud (WC2). The WC2 is a shared services offering that includes SaaS, PaaS and IaaS for meeting the public and extranet hosting needs of the Department of the Treasury and other Federal Agencies. As the prime contractor, Smartronix was able to deliver a robust, responsive and reliable solution that hosts multiple mission critical systems. Smartronix has ensured the successful operation and maintenance of the existing Treasury PCWS environment since 2010, which was the original contract that was subsequently recompeted and again awarded to Smartronix. The project scope includes providing managed cloud services and CMS management support for the SharePoint 2010 platform hosted on the AWS EC2 VPC platform. The WC2 offers a federated identity management capability along with TIC connectivity for protecting sensitive and PII data (unclassified). Smartronix supports more than a dozen websites on a variety of platforms including Windows, Linux and technologies including ASP, Java, Node.JS, SharePoint, HTML on IIS. The AWS services provided to Treasury include cloud computing services to support Application hosting (SharePoint, .NET and Java), Backup and storage (using S3 and snapshots), Web hosting (Apache, Microsoft IIS), Databases (SQLServer, MySQL) and various other utility services including load balancing across multiple AZ's and Regions. Smartronix also was responsible for incidence response with SLA's including detailed usage information including billing based on usage and reporting on virtual machines, storage and bandwidth consumed. The cloud computing services included delivering services over the East Geography and the West Region for DR. B
   The Treasury BPA is currently valued at approximately $45M
3. **Period of Performance:** 4/1/2013 – Ongoing

Consumer Financial Protection Bureau (CFPB)

1. **Contract Number:** GS-35F-0362J; TFSACFPBPA14004 (Services Calls 0001 and 0002)
2. **Description and Relevance:** Smartronix has supported Consumer Financial Protection Bureau's (CFPB) mission since the inception of the agency using Amazon Web Services (AWS) for providing a secure and rapidly expandable computing platform for hosting external and internal applications. The solution included the design and development of VPC enclaves, management and security & FISMA compliance services. The Smartronix Team actively supports multiple CFPB development and engineering teams with their cloud computing needs including supporting daily operations and executing maintenance tasks. CFPB has multiple segmented VPC within the AWS EC2 Platform that meet the needs of a variety of production and dev & test use case needs. Specific services provided by Smartronix include Cloud Infrastructure Systems Administration and Systems Engineering services in support of CFPB's private and public cloud hosting platforms including pCloud (Terremark), Amazon VPC and Akamai CDN. Key activities and services performed by Smartronix staff include:

- System Access Management: Provide VPN boundary support for administration of virtual machines in the Community Cloud enclave enabling RDP and SSH interface to Windows and Linux machines respectively. Establish Remote Desktop Gateway supporting secure RDP access to Window's based servers and access to multi-node Terminal Services Servers. Enable Directory Services with integrated DNS services across AZs. Provide an integrated self-service password change portal for site administrators and content managers.
- Security Management: Operate a scalable, redundant application and network layer firewall using Microsoft TMG for protection against Web-based threats, including URL filtering, antimalware inspection, HTTP/S inspection, and intrusion prevention. Provide security policy management using multiple antivirus solutions.
- Systems Monitoring - End to end monitoring using SolarWinds for health and performance statistics and alerting for IT services across the Windows and Linux environments
- Systems Management - Provide patch management for all Windows and Linux machines.
- File and Data Transfer – Operate primary and back-up SMTP servers in each availability zone and secure FTP services for file transfer in and out of the Cloud enclave.

3. **Period of Performance:** Jan 2011 - Ongoing

NIST

1. **Contract Number:** SB1341-14-SE-0423
2. **Description and Relevance:** Smartronix provides NIST with an experienced, professional, security-focused organization that advises and assists NIST in fulfilling their AWS needs. We advise NIST on challenges related to implementing cloud-based IaaS systems and services, which include public, private, and hybrid cloud systems and services using our deep capabilities in security and networking, and detailed and deep knowledge of government regulations – such as FISMA and FedRAMP. We also provide detailed billing information, which will facilitates chargeback capabilities. Our services provide NIST with on-demand self-service functionality, including provisioning, reporting, and billing functions.
3. **Period of Performance:** 10/1/14 - Ongoing

DOI FCHS BPA

1. **Contract Number:** D13PC00029
2. **Description and Relevance:** Description of Services/Products Provided: Smartronix is supporting DOI in their transformation from a vast and heterogeneous systems portfolio to a modern services based architecture. The cloud hosted services being delivered by Smartronix are supporting DOI's target to achieve $500 million in savings by 2020, which will significantly impact DOI's ability to provide essential services and achieve its mission objectives. In a budget-constrained environment, Smartronix has been able to provide technology capabilities that help overcome obstacles that DOI is facing, to include their challenging mission, geographical distribution, and complex organization.
   With more than 50% of DOI's IT budget currently directed to IT infrastructure, Smartronix has driven a focus on strategic and mission facing technologies. Smartronix has helped DOI to leave commoditized IT services to those providers who are experts in delivering cloud technologies with scope, scale, and cost efficiency. By implementing modern cloud-based IT at DOI, Smartronix is driving more predictable, transparent, and low cost capability which provides reduced cap-ex, faster time-to-market, better innovation, increased scale, enhanced security, improved SLAs, and an expanded service catalog.
   Team Smartronix has worked with DOI to create a set of "Cloud Foundation Services" which serve as the building blocks for the IT Transformation. Initial service lines for a solid core with which DOI immediately delivers value to stakeholders while also forming the base for future efforts. Smartronix is driving a phased and continual improvement which creates the momentum necessary to meet future mission goals. The combined Smartronix/DOI team have built a solid foundation upon which future cloud goals will be met. The outcome of these efforts include changing how IT adds value to the mission, changing how IT is budgeted and procured, and changing how IT is delivered to its customers.
   A major aspect of this strategy work is developing a mission-focused cloud services catalog that allows Bureaus and Offices to benefit from securely migrating services to the Cloud. It takes a strong team and trusted partner to deliver the Cloud Foundation components to make this effort a success.
   Team Smartronix has worked to meet DOI's objectives, including the following:

   - Improved availability, performance, and flexibility of datacenter services;
   - Reduced Total Cost of Ownership ("TCO") of delivering IT services;
   - Promote the use of Green IT by reducing the overall energy, real estate footprint, and use of toxic components of DOI datacenters, and implementing effective recycling and reuse programs;
   - Ensure all applicable federal information security and privacy regulations are maintained;
   - Provide tiered functions, service levels, and performance for customers;
   - Provide interoperable and portable solutions that enable mobility across hosting models and service providers; and
   - Enable scaling of infrastructure and application resources to meet evolving application and user demand.

Team Smartronix has supported these objectives by providing best of breed, secure cloud services and expert associated support services. Our team delivered solutions which met and exceeded DOI's stated objectives. Quite simply, our cloud solutions are about delivering business agility, flexibility and transparency. We offer highly secure compute capacity on-demand via rapid provisioning allowing you to conserve power, optimize your use of datacenter space, simplify your IT infrastructure, and enabled staff to be as productive as possible.

3. **Period of Performance:** 8/18/12 - Ongoing

4.3. FINANCIALS (RFP 6.3)

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Smartronix' complete audited financial statements for 2013 and 2014 are attached. Smartronix' Dun and Bradstreet is 965091606.

4.4. GENERAL INFORMATION (RFP 6.4)

4.4.1. Solution Information (RFP 6.4.1)

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

AWS Differentiators: Below are some features and benefits of AWS that set our cloud infrastructure services apart:

Pace of Innovation: AWS's pace of innovation is funded and sustained through our economies of scale and commitment to delivering the products and services that matter most to our customers. Our approach to product development and delivery is fundamentally different than that of other Cloud Service Providers (CSPs). We have decentralized, autonomous development teams that work directly with customers. They are empowered to autonomously develop and launch new features based on what they learn from interactions with both commercial and public sector customers. AWS's continual innovation ensures that customers maintain state-of-the-art IT infrastructure without having to make recapitalization investments. As of January 1, 2016, AWS has launched a total of 1,896 new services or major features since inception in 2006 (including 516 in 2014 and 722 in 2015). According to the Gartner, Inc. 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide, "AWS is a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market."

Service Breadth and Depth: AWS offers the broadest set of global compute, storage, networking, database, analytics, application, deployment, management, and mobile services that help organizations move faster, lower IT costs, and scale applications. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 50 services that serve over one million active customers in more than 190 countries through our 12 regions, 32 Availability Zones, and 54 Edge Locations. Gartner Inc. reported in its 2015 Magic

Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report that AWS "has the richest array of IaaS features," "continues to rapidly expand its service offerings and offer higher-level solutions," and has "over 10 times more cloud IaaS compute capacity in use than the aggregate total of the other 14 providers in this Magic Quadrant."

Partner and Software Ecosystem: According to the Gartner, Inc. 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report, AWS has attracted "a very large technology partner ecosystem that includes software vendors that have licensed and packaged their software to run on AWS, as well as many vendors that have integrated their software with AWS capabilities. It also has an extensive network of partners that provide application development expertise, managed services, and professional services such as data center migration." AWS has thousands of organizations in the AWS Partner Network (APN) including system integrators, consulting firms, and independent software vendors (ISVs). AWS Marketplace, an online software store, helps customers search over 2,300 listings to buy and immediately start using software that runs on AWS.

AWS Cloud Security Authorizations and Experience: AWS offers customers a powerful cloud security capability based on cutting-edge security experience and backed by an extensive repertoire of accreditations and authorizations. In The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014 report, Forrester Research named AWS as the only provider in the Leader category. Forrester stated, "AWS leads the pack. AWS demonstrated not only a broad set of security capabilities in data center security, certifications, and network security, but also excelled in customer satisfaction, security services partnerships, and a large installed base." AWS has achieved two Provisional Authorizations to Operate (P-ATOs) for mission systems designated by DISA as Cloud Computing Security Requirements Guide (SRG) level 2 (covering all AWS regions in the contiguous United States [CONUS]) and SRG level 4 (covering only the AWS GovCloud (US) Region).

AWS Pricing: As AWS's cloud computing infrastructure grows, it gains efficiency and economies of scale, which we pass on to our customers in the form of lower prices. The Gartner, Inc. 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report states that AWS has "over 10 times more cloud IaaS compute capacity in use than the aggregate total of the other 14 providers," demonstrating how AWS's massive economies of scale make it possible to lead the cloud market in lowering prices. The AWS strategy of pricing each service independently gives customers tremendous flexibility to choose the services they need for each project and to pay only for resources used. The economies of scale available with the cloud, and the massive scale at which we operate, allows AWS to constantly purchase and refresh large volumes of infrastructure at very low cost. Consequently, AWS customers reap the benefits of decreased IT costs such as better performance through improved quality and availability of IT infrastructure and enhanced functionality through system-wide innovation in the AWS IaaS platform.

Business Benefits of AWS Cloud Services

There are additional business benefits that AWS cloud services can help customers realize. A few of these are listed here:

Almost Zero Upfront Infrastructure Investment: If a customer wants to build a large-scale system, it may cost a fortune to invest in real estate, physical security, hardware (racks, servers, routers, backup power supplies), hardware management (power management, cooling), and operations personnel. Because of the high upfront costs, the project would typically require several

rounds of management approvals before the project could even get started. With AWS's utility-style cloud computing, there is no fixed cost or startup cost.

Just-In-Time Infrastructure: In the past, if an application became popular and a business' systems or infrastructure did not scale, it became a victim of its own success. Conversely, if a developer invested heavily and did not get popular, it became a victim of failure. By deploying applications in the AWS cloud with just-in-time self-provisioning, customers do not have to worry about pre-procuring capacity for large-scale systems. AWS's cloud increases agility, lowers risk, and lowers operational cost, because customers can scale cloud resources as they grow and only pay for what they use.

More Efficient Resource Utilization: System administrators usually worry about procuring hardware (when they run out of capacity) and higher infrastructure utilization (when they have excess and idle capacity). With AWS, they can manage resources more effectively and efficiently by having the applications request and relinquish resources on-demand.

Usage-Based Costing: With utility-style pricing, AWS customers are billed only for the infrastructure that has been used. AWS customers do not pay for allocated but unused infrastructure. This adds a new dimension to cost savings, allowing customers to see immediate cost savings when they deploy an optimization patch to update their cloud application. For example, if a caching layer can reduce data requests by 70%, the savings begin to accrue immediately. Moreover, if customers build platforms on the cloud, they can pass on the same flexible, variable usage-based cost structure to their own customers.

Reduced Time to Market: Parallelization is the one of the great ways to speed up processing. If one compute-intensive or data-intensive job that can be run in parallel takes 500 hours to process on one machine, with cloud architectures, it would be possible to spawn and launch 500 instances and process the same job in 1 hour. Having available an elastic infrastructure provides the application with the ability to exploit parallelization in a cost-effective manner reducing time to market.

Technical Benefits of AWS Cloud Services

Some of the key technical benefits of the AWS cloud are:

Automation – "Scriptable Infrastructure": AWS customers can create repeatable build and deployment systems by leveraging programmable (API-driven) infrastructure.

Auto Scaling: AWS customers can scale their applications up and down to match unexpected demand without any human intervention. Auto Scaling encourages automation and drives more efficiency.

Proactive Scaling: Customers can scale applications up and down to meet anticipated demand with proper planning of traffic patterns so that costs remain low while scaling.

More Efficient Development Lifecycle: Production systems may be easily cloned for use as development and test environments. Staging environments may be easily promoted to production.

Improved Testability: Never run out of hardware for testing. Inject and automate testing at every stage during the development process. AWS customers can spin up an "instant test lab" with pre-configured environments only for the duration of testing phase.

Disaster Recovery and Business Continuity: The cloud provides a lower cost option for maintaining a fleet of disaster recovery servers and data storage. With the cloud, customers can take advantage of geo-distribution and replicate the environment in other locations within minutes.

Overflow Traffic to the Cloud: With a few clicks and effective load balancing tactics, customers can create a complete overflow-proof application by routing excess traffic to the cloud.

4.4.2. Auditing capabilities and Reports (RFP 6.4.2)

Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Smartronix is SOC 1, SOC 2, ISO 9001, ISO 20001, and CMMI Level 3.

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)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001
- ISO 27017
- ISO 27018
- ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) security impact levels 2 and 4
- 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)

4.5. BILLING AND PRICING PRACTICES (RFP 6.5)

4.5.1. Billing and Pricing Practices (RFP 6.5.1)

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

Smartronix will bill for actual usage of all services used in any given month at AWS's then-current prices. For current prices for AWS services, please refer to the AWS website at http://aws.amazon.com

Smartronix can generate detailed billing reports that break down costs by the hour, day, or month; or by each account in your organization; or by product or product resource, or by tags that you define yourself.

You might choose to receive detailed billing reports in order to do any of the following:

- Bring your billing data into an application that can read a CSV file.
- Build an application that uses your billing data.
- Monitor your month-to-date charges.
- Forecast your monthly charges.
- Share your data with a partner.
- Import your billing data into your accounting system.
- Retrieve your bill for multiple accounts.

Smartronix can help you customize these reports to list the AWS resources that generate the included charges, and create tags for your AWS resources to add your own labels to nearly every line item in your reports. You can view these reports in applications that can read CSV files, such as Microsoft Excel, or you can write custom applications that import the billing data from the file for analysis.

With Smartronix and AWS, customers can incorporate a utility-style pricing model, only paying for the resources consumed. AWS continues to lower the cost of cloud computing for its customers. In 2014, AWS reduced the cost of compute by an average of 30%, storage by an average of 51%, relational databases by an average of 28%, and this will continue to drive down the cost of customer IT infrastructure. The utility-style pricing model is explained below:

Pay as You Go: No minimum commitment or long-term contract is required. Customers can turn off cloud resources and stop paying for them when they are not needed, maximizing Return on Investment (ROI) through full utilization.

Pay Less When You Reserve: For certain AWS products, customers can invest in reserved capacity with Smartronix, paying a low up-front fee to receive a significant discount. This results in overall savings of up to 60% (depending on the type of instance reserved) over equivalent on-demand capacity.

Pay Even Less Per Unit by Using More: AWS pricing is tiered for storage and data transfer, so the more customers use, the less they pay per gigabyte.

Pay Even Less as AWS Grows: AWS continually focus on reducing data center hardware costs, improving operational efficiencies, lowering power consumption, and passing savings back to customers. AWS has a history of continually lowering prices and has reduced prices 51 times since AWS launched in 2006. Smartronix passes these savings along to our customers automatically based on our billing model.

Transparency: Smartronix and AWS provides transparent, publicly available, and up-to-date pricing, and tools that allow customers to evaluate AWS pricing against other Cloud Service Providers (CSPs). AWS's Simple Monthly Calculator can be found at http://calculator.s3.amazonaws.com/index.html.

Governance: Smartronix provides tools to generate detailed and customizable billing reports to meet customer business and compliance needs. Additionally, Smartronix can

help customers manage and control cost utilization/tracking tools in order to provide customized billing reports.

Smartronix can help customers compare AWS to the cost of running applications in an on-premises or traditional hosting environment. Further, Smartronix can help to provide Total Cost of Ownership comparisons between different models of computing. Analysis shows that AWS offers significant cost savings (up to 80%) compared to equivalent on-premises deployments.

Potential Business Value of Running Applications on AWS

- Five year ROI: 560%
- Payback period: 5.5 months
- $1.54M average five-year discounted business benefits per application
- 64.3% lower TCO
- 68.1% more efficient IT staff operations
- $76,800 additional revenue per year per application
- 118.4% more applications delivered
- 81.7% less downtime

Source: *IDC Whitepaper, sponsored by AWS, "Quantifying the Business Value of Amazon Web Services," May 2015.* http://d0.awsstatic.com/analyst-reports/IDC_Business_Value_of_AWS_May_2015.pdf.

Figure 8: Business Value of AWS

AWS is a highly cost-effective alternative to on-premises infrastructure solutions, delivering significantly reduced IT system and management costs. In 2015, AWS commissioned the International Data Corporation (IDC) to interview 11 organizations that deployed applications on AWS. IDC set out to understand the long-term economic implications of moving workloads onto Amazon cloud infrastructure services, the impact of moving applications on developer productivity and business agility, and the new opportunities that businesses could address by moving resources onto AWS.

IDC discovered that developing, deploying, and managing critical applications in AWS delivered a five-year TCO savings of 64.3% when compared with deploying the same resources on-premises or in hosted environments. The findings also showed a 560% ROI over five years.

Consolidated Billing

You can also use the Consolidated Billing feature to consolidate payment for multiple AWS accounts within your organization by designating one of them to be the payer account. With Consolidated Billing, you can see a combined view of AWS charges incurred by all accounts, as well as get a detailed cost report for each individual AWS accounts associated with your payer account. Consolidated Billing is offered at no additional charge from Smartronix.

4.5.2. Identify cost impacts (RFP 6.5.2)

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

There are multiple cost impacts to consider when implementing a cloud solution. The first is to understand the billing types and their ramifications on cost. Its important to know how prepaid Reserved Instances work. With RI's the account is charged for 100% utilization of that reservation versus on demand which can be shut down but come with a higher hourly rate. Smartronix has a team of experts to help our customers navigate these decisions and will walk you thru the

purchasing process. We also offer the CloudCheckr cost portal at no additional charge to assist the customer in running reports and to better understand their current and historical AWS spend.

The next cost impact is the opportunity cost of not embracing automation. Smartronix employees a DevOps team that has developed scripts to automatically shutdown instances that can be run on a schedule. Through automation we can shut down instances that are idle during scheduled time period (ie nights and weekends). This can give the customer cost savings greater than purchasing Reserved Instances or staying in a pure on-demand model.

Another potential cost impact is the lack of mature business rules and policies around who may have access to deploy instances or wrong sizing. As a part of the Smartronix CAMS offering we have policies, such as change control, to help customers develop their access policies to keep the size and growth of the infrastructure within the cost structure.

Additionally, we recommend strong governance and workflows around the provisioning process which include establishing cost transparency plans and frequent billing alerts when thresholds have been met.

4.5.3. NIST compliance (RFP 6.5.3)

Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

As related to billing and pricing practices, the services are NIST compliant in the following ways:

- All services are Pay Per Use
- All services are available on demand
- Services are web accessible
- Network services are ubiquitous
- All services are logically or physically isolated per customer
- Capacity is near infinite with no delays for expanding services
- Services can be shut down without incurring additional charges

The technical discussion of NIST compliance is in Section 6.

4.6. SCOPE AND VARIETY OF CLOUD SOLUTIONS (RFP 6.6)

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

The following chart outlines the full scope of AWS Services we are offering across IaaS, PaaS, and SaaS service models available across all deployment methods.

Figure 9: Entire AWS Service Catalog including Infrastructure, Platform, and Software Services

IaaS Services

These services include the core compute, storage and network components that make up AWS EC2 including the security, monitoring, encryption, desktop, and underlying server infrastructure.

PaaS Services

These services include all of the platform components that manage the underlying AWS server infrastructure for you including EMR (Hadoop), Relational Database Services, Elastic Container Services, Elastic Beanstalk, and DevOps tools.

SaaS Services

These services include all of the readily available software services supporting messaging, collaboration, search, and analytics services.

The service models on AWS blur across service boundaries as all services run on the underlying IaaS cloud infrastructure. The deployment methods are straightforward as AWS supports Private (dedicated), Public, Community (GovCloud), and hybrid extension capabilities.

AWS Hybrid Model (Extend IT Services)

A hybrid cloud environment allows organizations to address immediate IT needs though utilizing the benefits of cloud computing, while also retaining on-premises infrastructure. A hybrid model is a prudent approach to cloud adoption for organizations that require the immediate use of scalable cloud services, but are not ready to fully migrate all application and workloads to the cloud.

AWS provides the tools and solutions to integrate existing on-premises resources with the AWS cloud. By using AWS to enhance and extend your capabilities, without giving up the investments you have already made, you can accelerate your adoption of cloud computing.

General Hybrid Cloud Requirements and Issues: Some of the common requirements and issues associated with hybrid cloud are:

- On-demand, scalable compute resources.
- Flexible, secure, and reliable network connectivity.
- Automated backup and recovery.
- A highly secure and controlled platform, with a wide array of additional security features.
- Integrated access control.
- Easy-to-use management tools that integrate with on-premises management resources.

AWS Capabilities for Hybrid Cloud Solutions: AWS provides all of the capabilities required for a dynamic, reliable, and secure hybrid cloud solution:

Extend Network Configuration: Flexible network connectivity is a cornerstone of integrating distributed environments, including AWS and your existing on-premises equipment. With Amazon VPC, you can extend your on-premises network configuration into your virtual private networks on the AWS cloud. AWS resources can operate as if they are part of your existing corporate network. Amazon VPC lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Integrated Cloud Backups: AWS helps simplify the backup and recovery environment for the enterprise. You can leverage the on-demand nature of the cloud and automate your backup and recovery processes so they are not only less complex and lightweight, but also easy to manage and maintain. Storage services with AWS are designed to provide 99.999999999% durability, so you can feel confident your backups are protected.

Integrated Network Connection: On-premises connection with AWS is best accomplished with AWS Storage Gateway, a software appliance installed in your data center with cloud-based storage to provide seamless and secure integration between an organization's existing IT environment and the AWS storage infrastructure. Using industry-standard storage protocols, the service allows you to store data in the AWS cloud for scalable and cost-effective storage. It provides low-latency performance by maintaining frequently accessed data on-premises while securely storing all of your data encrypted in the Amazon Simple Storage Service (Amazon S3) or Amazon Glacier.

Integrated Resource Management and Workload Migration: All AWS cloud services are driven by robust APIs that allow for a wide variety of monitoring and management tools that integrate easily with your AWS cloud resources. It's likely that many of the tools that your organization is using to manage your on-premises environments can be extended to include AWS

as well. Integrating your AWS environment can provide a simpler and quicker path for cloud adoption, because your operations team does not need to learn new tools or develop completely new processes.

Solution Use Cases: Use cases for AWS hybrid solutions include:

- Migrating workloads and data that are "cloud ready" (i.e., applications that do not need significant re-architecting for a cloud migration).
- Retaining data on-premises to meet regulatory and compliance needs.

Hybrid Cloud Resources: AWS provides the tools, information, and guidance to build a hybrid cloud environment that can offer an immediate impact to customers.

Along with the full AWS Service Catalog, Smartronix is offering its Cloud Assured Professional and Managed Services for designing, deploying, migrating, operating, and managing compliant environments on AWS. These services are described in greater detail below.

4.7. BEST PRACTICES (RFP 6.7)

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Smartronix works primarily in heavily regulated and security compliance driven domains such as the government, Healthcare, Financial Services, and Department of Defense. We based our CloudAssured Managed Services capability on NIST 800-53: Rev 4 to meet the FedRAMP standards and have been through all of the requisite 3PAO audits for ensuring our controls meet the standards for confidentiality, integrity, and availability.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation. AWS's highly secure data centers use state-of-the-art electronic surveillance and multi-factor access control systems and maintain strict, least-privileged-based access authorizations. Our environmental systems are designed to minimize the impact of disruptions to operations, and our multiple geographic regions and Availability Zones allow customers to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS manages over 1,800 security controls to provide an optimally secure environment for all of our customers.

In addition, network traffic between AWS regions, Availability Zones, and individual data centers travels over private network segments by default. These private network segments are fully isolated from the public Internet and not routable externally. AWS resources can be configured to reside only on isolated AWS network segments and to avoid utilizing any public IP addresses or routing over the public Internet.

AWS security engineers and solution architects have developed whitepapers and operational checklists to help customers select the best options for their needs and to recommend security best practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

Built-In Security Features
Not only are applications and data protected by highly secure facilities and infrastructure, they are also protected by extensive network and security monitoring systems. AWS and its partners offer

over 700 tools and features to help customers meet their security objectives concerning visibility, auditability, controllability, and agility. These tools and features provide basic but important security measures such as Distributed Denial of Service (DDoS) protection and password brute-force detection on AWS accounts. AWS-provided security features include:

Secure Access – Customer access points, also called Application Programming Interface (API) endpoints, allow secure HTTP access (HTTPS) so that customers can establish secure communication sessions with their AWS cloud services using Secure Socket Layer (SSL)/Transport Layer Security (TSL).

Built-In Firewalls – Customers can control how accessible their instances are by configuring built-in firewall rules—from totally public to completely private or somewhere in between. And when instances reside within an Amazon Virtual Private Cloud (Amazon VPC) subnet, customers can control egress as well as ingress.

Unique Users – The AWS Identity and Access Management (IAM) tool allows AWS customers to control the level of access their own users have to AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.

Multi-Factor Authentication (MFA) – AWS provides built-in support for MFA for use with AWS accounts as well as individual AWS IAM user accounts.

Private Subnets – The Amazon VPC service allows customers to add another layer of network security to instances by creating private subnets and even adding an Internet Protocol Security (IPsec) Virtual Private Network (VPN) tunnel between a home network and Amazon VPC.

Encrypted Data Storage – Customers can have the data and objects they store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.

Dedicated Connection Option – The AWS Direct Connect service allows customers to establish a dedicated network connection from their premises to AWS. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS cloud.

Isolated GovCloud – For customers who require additional measures in order to comply with US International Traffic in Arms Regulations (ITAR), AWS offers an entirely separate region called AWS GovCloud (US). This isolated region provides an environment where customers can run ITAR-compliant applications and provides special endpoints that utilize only Federal Information Processing Standard (FIPS) 140-2 encryption.

Dedicated, Hardware-Based Crypto Key Storage Option – For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.

Centralized Key Management – For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.

Perfect Forward Secrecy – For even greater communication privacy, several AWS cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.

Several of AWS's built-in cloud security features focus on providing visibility into data, performance, and resource usage. The tools listed below help customers gain more insight into their cloud operations, giving them the means to better control their security and providing information for data-driven decisions.

AWS Trusted Advisor – Provided automatically when AWS customers sign up for premium support, the AWS Trusted Advisor service is a convenient way for customers to see where they could use a little more security. It monitors AWS resources and alerts customers to security configuration gaps such as overly permissive access to certain Amazon Elastic Compute Cloud (Amazon EC2) instance ports and Amazon S3 storage buckets, minimal use of role segregation using AWS IAM, and weak password policies.

Amazon CloudWatch – Amazon CloudWatch enables customers 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 a 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, using these insights to react intelligently and keep applications running smoothly.

AWS CloudTrail – AWS CloudTrail provides logs of all user activity within an AWS account. 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. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

AWS Config – With the AWS Config service, customers can immediately discover all of their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.

More information on these and other features is available at http://aws.amazon.com/security/aws-security-features/.

Third-Party Security Tools

We also offer additional third-party security tools to complement and enhance our customers' operations in the AWS cloud. AWS Partner Network (APN) partners offer hundreds of familiar and industry-leading products that are equivalent to, identical to, or integrate with existing controls in a customer's on-premises environments. Customers can browse and purchase APN partner products on the AWS Marketplace. These products complement existing AWS cloud services to enable customers to deploy a comprehensive security architecture and a more seamless experience across their cloud and on-premises environments. The APN partner security products cover multiple areas of security, including application security, policy management, identity management, security monitoring, vulnerability management, and endpoint protection. Below,

Figure 10 is a snapshot of the APN partners and categories of products available under the security category in the AWS Marketplace.

Figure 10: The AWS Marketplace provides access to many familiar and trusted security vendors

Several of the security products that AWS offers are provided only by APN partners that are prequalified by the APN Partner Competency Program, which confirms their technical proficiency and proven customer success in specialized solution areas. AWS's Security Competency Partners can also provide demos and consulting services that are not always available through the AWS Marketplace.

5. ORGANIZATION PROFILE (RFP 7)

5.1. CONTRACT MANAGER (RFP 7.1)

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have experience managing contracts for cloud solutions.

Smartronix contract manager is Melinda Armsworthy

5.1.1. Contract Manager Information (RFP 7.1.1)

Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Melinda Armsworthy, 301-373-6000 x314, marmsworthy@smartronix.com, M-F 8:30 5:00 Eastern

5.1.2. Experience in Contract Management (RFP 7.1.2)

Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

Ms. Armsworthy has over 15 years of experience performing contract administration and program analysis support. She provides cradle to grave contract management for extremely large multi-year contracts, program management support for pre- and post-award contract phases, and financial management/analysis and support. She possess well-developed planning and organizational skills, able to work as a team member or independently, and able to work efficiently in a fast-paced environment.

5.1.3. Contract Manager Roles and Responsibilities (RFP 7.1.3)

Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

Ms. Armsworthy is responsible for the negotiation, administration, and execution of contracts; contractual deliverables and financial reporting; and participates in proposal development and pricing. Ms. Armsworthy is an integral member of the Smartronix Government-wide Acquisition Contract (GWAC) Program Management Office (PMO). Ms. Armsworthy assists the Contracts Director with all aspects of the daily operations of the Contracts and Pricing departments, leads the team members, and ensures accuracy and compliance with all company policies and procedures. She acts as the liaison and back-up when the Director is unavailable. Ms. Armsworthy provides consistent leadership to the contracts staff to ensure effective and efficient contract administration of assigned programs and oversees the contracts and pricing team in daily responsibilities and ensures accurate and timely completion of tasking. Ms. Armsworthy works with team members, management, and the owners and consistently maintains the highest standards of professionalism.

6. TECHNICAL RESPONSE (RFP 8 ATTACHMENTS C&D)

A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response. Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

6.1. TECHNICAL REQUIREMENTS (RFP 8.1)

6.1.1. Identify Cloud service and deployment (RFP 8.1.1)

Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

We have elected to provide AWS IaaS, PaaS, and SaaS service models covering each deployment model (private, public, community, and hybrid.) and at all FIPS 199 data classification levels (Low Impact through High).

Although AWS is primarily considered a public cloud IaaS/PaaS solution provider there are services related to email, collaboration, search, workflow, messaging, and business intelligence that most closely resemble SaaS offerings by the NIST model definition. Additionally, Smartronix provides a robust set of Managed Services that extend across all service models.

Private cloud services are provided through AWS Virtual Private Cloud technology utilized dedicated hosts. Community cloud services are provided to government customers and entities utilizing AWS GovCloud. Public cloud deployment methods utilize AWS Virtual Private Cloud technologies running on multitenant (logically isolated) infrastructure. There are also hybrid capabilities offered by AWS that extend services onto on-premises infrastructure that will be provided as well.

6.1.2. Solution Compliance with NIST characteristics (RFP 8.1.2)

For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following Characteristics, as defined in NIST Special Publication 800-145:

6.1.2.1. NIST Characteristic - On-Demand Self-Service (RFP 8.1.2.1)

Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

Amazon Web Services, Inc. (AWS) provides customers of all sizes with on-demand access to a wide range of cloud infrastructure services, charging you only for the resources you actually use. AWS enables you to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our customers can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000

servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it simple for customers to get started and be productive.

This characteristic is met for all AWS services spanning IaaS, PaaS, and SaaS services.

6.1.2.2. NIST Characteristic - Broad Network Access (RFP 8.1.2.2)

Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

AWS provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application, mobile client, or programmatically through published and well documented APIs.

This characteristic is met for all AWS services spanning IaaS, PaaS, and SaaS services. All AWS PaaS and SaaS services reside on the underlying AWS IaaS cloud infrastructure.

6.1.2.3. NIST Characteristic - Resource Pooling (RFP 8.1.2.3)

Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

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 y an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010.

This characteristic is met for all AWS services spanning IaaS, PaaS, and SaaS services. PaaS services such as Relational Database Services and Elastic Container Services pull from a global resource pool but maintain logical isolation of services. SaaS services such as AWS WorkMail maintain logical isolation.

6.1.2.4. NIST Characteristic - Rapid Elasticity (RFP 8.1.2.4)

Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand. Customers need to be confident that their existing infrastructure can handle a spike in traffic and that the spike will not interfere with normal business operations. Elastic Load Balancing and Auto Scaling can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases.

This characteristic is met for all AWS services spanning IaaS, PaaS, and SaaS services. PaaS services such as Elastic Beanstalk and Elastic Container Services automatically scale up and down based on demand for services. SaaS services such as AWS WorkMail scale up to support additional users automatically.

6.1.2.5. NIST Characteristic - Measured Service (RFP 8.1.2.5)

Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

The AWS infrastructure provides service metrics for services such as storage, compute, and bandwidth that enable the automatic control of resource utilization. These metrics are provided via AWS CloudWatch and can be programmatically used to trigger resource scaling, alerts, billing events, and operations support.

AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

6.1.3. Sub Categories for each solution IaaS/PaaS/SaaS (RFP 8.1.3)

Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

The following chart outlines the full scope of AWS Services we are offering across IaaS, PaaS, and SaaS service models available across all deployment methods.

Figure 11: Entire AWS Service Catalog including Infrastructure, Platform, and Software Services

IaaS Services

These services include the core compute, storage and network components that make up AWS EC2 including the security, monitoring, encryption, desktop, and underlying server infrastructure.

PaaS Services

These services include all of the platform components that manage the underlying AWS server infrastructure for you including EMR (Hadoop), Relational Database Services, Elastic Container Services, Elastic Beanstalk, and DevOps tools. These services are listed in the Platform Services diagram above.

SaaS Services

These services include all of the readily available software services supporting messaging, collaboration, search, and analytics services. These service include AWS WorkMail, AWS WorkDocs, and CloudSearch.

The service models on AWS blur across service boundaries as all services run on the underlying IaaS cloud infrastructure. The deployment methods are straightforward as AWS supports Private (dedicated), Public, Community (GovCloud), and hybrid extension capabilities.

6.1.4. Compliance with Attachments C&D (RFP 8.1.4)

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

Smartronix will comply with the NIST Service Models, Deployment Methods, and Scope of Services outlined in Attachment C&D. These services are core to cloud delivery and service intermediation for Smartronix and AWS.

6.1.5. Scope of Services (RFP 8.1.5)

As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

As described in RFP 8.1 through 8.4, the AWS service model enables ubiquitous, convenient, on-demand network access to a vast pool of configure cloud resources that can be rapidly provisioned and released without service provider interaction. AWS offers capabilities that are self-service or that can be managed by a third party broker and Managed Services Partner such as Smartronix.

6.2. SUBCONTRACTORS (RFP 8.2)

6.2.1. Direct/Indirect Solutions (RFP 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.

Smartronix intends to provide all cloud solutions directly without the use of Subcontractors. Smartronix has a dedicated cloud practice that can currently meet all of the requirements listed in the RFP.

6.2.2. Extent (RFP 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.

As stated above, Smartronix intends to provide all cloud solutions directly without the use of Subcontractors. Smartronix has a dedicated cloud practice that can currently meet all of the requirements listed in the RFP.

6.2.3. Subcontractor qualifications (RFP 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.

As stated above, Smartronix intends to provide all cloud solutions directly without the use of Subcontractors. Smartronix has a dedicated cloud practice that can currently meet all of the requirements listed in the RFP.

6.3. WORKING WITH PURCHASING ENTITIES (RFP 8.3)

6.3.1. Purchasing Entities engagement (RFP 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.

Smartronix currently has been ITSM certified with ISO:20001v2011 which includes ITIL based Incident Management procedures. The following outlines our Incident Response process:

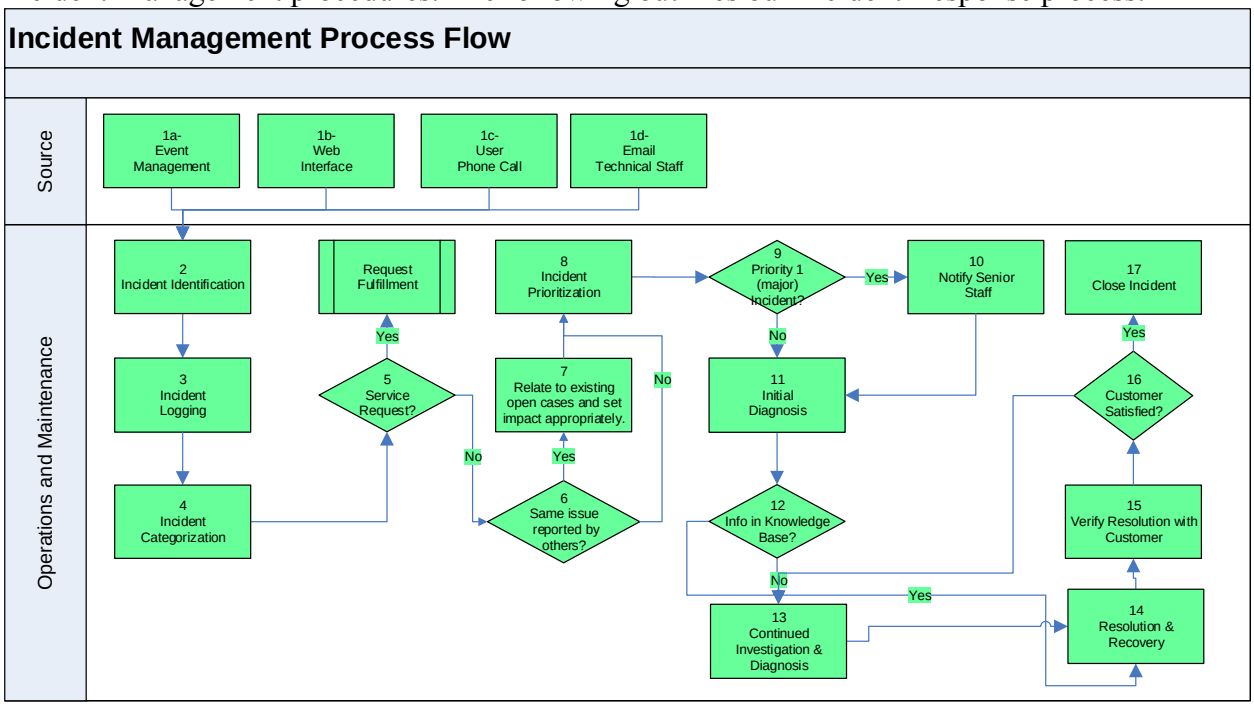


Figure 12: Incident Management Process

Incident Management Process Flow Steps

Role	Step	Description
SMX Customer	➢	Incidents may be discovered by the customer or technical staff through various means, i.e., phone, email, or a self-service web interface. Incidents may also be reported through the use of automated tools performing Event Management.
SMX Cloud Assured O&M Team	➢	**Incident identification** The O&M team may be alerted to an Incident via monitoring tools (EM7, Pingdom for example), or by a customer report through the customer portal, phone call, or email
	➢	**Incident logging** All Incidents will be recorded in the ServiceNow ticketing system. An Incident ticket must be created for every incident
	➢	**Incident categorization** The affected service is to be identified from the Service Catalogue; select from the Category drop-down menu on the ticket face
	➢	Select the sub-category to further define the item affected. Sub-categories are directly related to the Category type.
	➢	**Incident prioritization** Ticket priority will be assigned based on the CAMS Severity matrix. It may be adjusted at the request of a customer escalation and requires manager approval
	➢	**Urgency:** Select appropriate urgency type based on business impact
	➢	**Priority:** Selection drive division of workload the team. Highest priority gets worked first. See Severity Matrix.
	➢	**Contact Type**: Default = Self-service. Record the method of Incident discovery from the drop-down menu
	➢	**Status:** All tickets appear in NEW status when created. Change Status to Active once ticket is assigned to a specific tech.
	➢	**Assignment Group:** All tickets are automatically assigned to the O&M group when opened. The ticket will stay within the O&M team unless it is determined that an escalation to the SA team is required. If so, change the Assignment Group to **SA,** select from the drop-down menu.
	➢	**Assigned to:** Ticket queue manager will review the ticket and assign to the appropriate O&M tech for triage and diagnosis. Select the Tech from the drop-down menu.

Role	Step	Description
	➢	**Company:** Make sure the Company name is populated with the appropriate Company, from the drop-down menu.
	➢	**Short Description:** Enter a short description that accurately reflects the nature of the Incident. Include the name/Date in the field. This will be used as a reference for communications and notifications
	➢	**Description:** Enter detailed description of the problem. Include specifics around server, service, applications, etc. As well as log info, copy of alert or records from the customer.
	➢	**Notifications:** For all Priority 1 incidents, management notification should occur immediately to insure appropriate resources are made available.
	➢	Notifications to the customer will be made based on intervals defined in the severity and notification matrix. These will occur whether it be automated within SN or manual via email
	➢	**Initial diagnosis** The O&M Team analyst will conduct initial diagnosis, using diagnostic scripts and known error information to determine possible cause of issue. The O&M Team will utilize the collected information to initiate a search of the Knowledge Base to find an appropriate solution. When possible, the O&M Team Analyst will resolve the incident and close the incident.
	➢	**Ticket note updates:** The O&M technical will provide ticket note updates at the intervals specified in the matrix, which are relative to ticket priority. All troubleshooting details will remain in the WORK NOTES field.
	➢	**Additional Comments (Customer Visible).** The O&M tech is responsible to enter status updates intended for the customer in this field. All notes must be suitable for customer viewing, and will be entered at regular intervals according to ticket priority.
	➢	**Ticket Resolution:** Once the ticket is resolved, the Assigned to Tech will change the STATUS field to RESOLVED.
	➢	The O&M team will inform the customer that the issue has been resolved and ask for confirmation. Once confirmed, the ticket can be moved to a CLOSED state.
	➢	**CLOSURE INFORMATION**: The Close Code and CLOSE NOTES fields are mandatory prior to ticket closure. These must be populated correctly before a ticket can be physically closed.

Role	Step	Description
	➢	**User satisfaction survey**. A survey will be sent to the customer once monthly by ServiceNow if they experienced an incident. Those metrics will be monitored (future feature).
	➢	**Ongoing or recurring problem?** Determine whether the incident is likely to recur and decide whether any preventive action is necessary to avoid this. Create a Problem Record and link the incident(s) in Problem Management, in all such cases so that preventive action is initiated and assign to a tier 2 or 3 team member.

Incident Escalation

Ownership of incidents always resides with the O&M Team. As a result, the responsibility of ensuring that an incident is escalated when appropriate also resides with the O&M Team.

The O&M team will monitor all incidents, and escalate them based on the following guidelines:

Priority	Time Limit before Escalation	
3 - Low	24 hours	Manager
2 - Medium	4 hours	Manager
	If on-call contact cannot be reached during non-business hours	Manager
	If neither on-call contact or their manager cannot be reached during non-business hours	Director
	12 hours	Director
1 - High	Immediate	Manager
	Immediate	Director

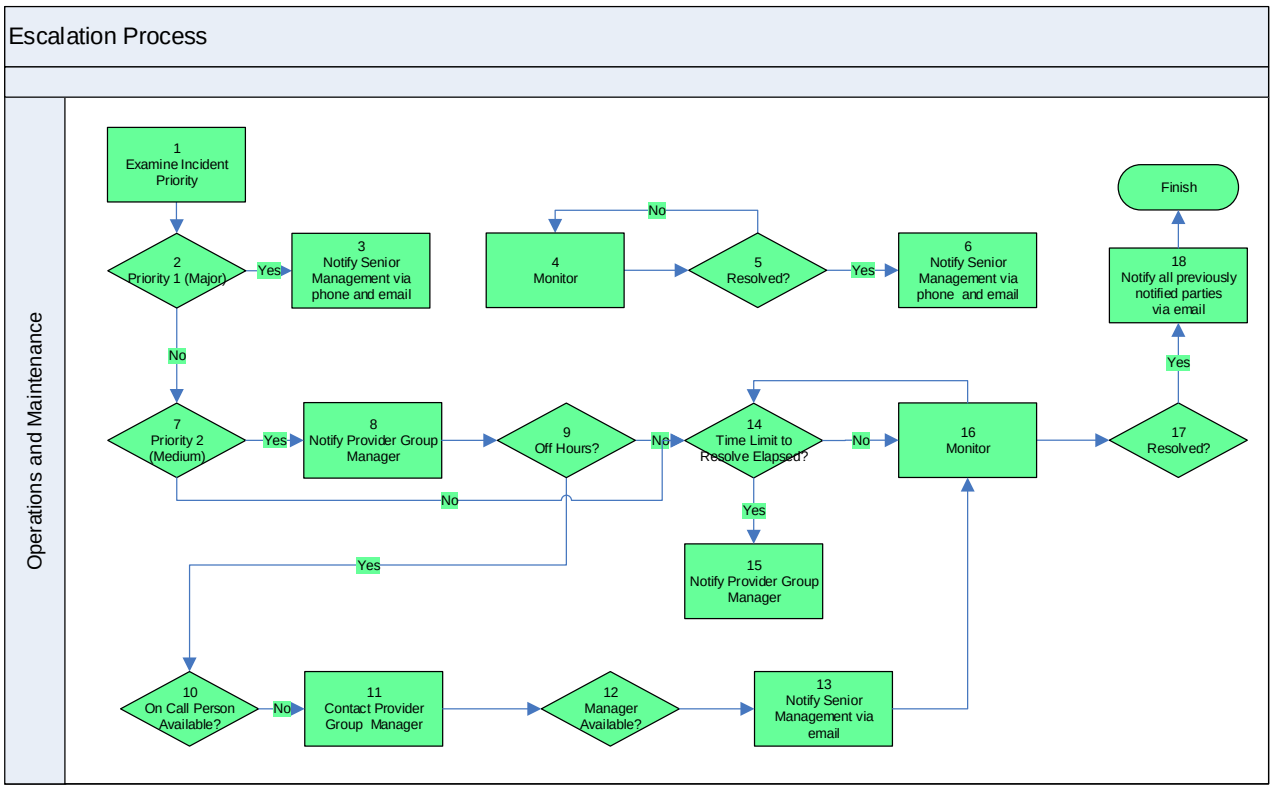


Figure 13: Escalation Process

Any time a case is escalated, notification will occur to various individuals or groups depending upon the priority of the incident. Following are basic guidelines for notifications:

- The default mechanism for notification will be by email unless otherwise specifically stated.

Whenever escalation or notification by phone is indicated, all known numbers for contact should be utilized, leaving voice mail on each until the support staff is contacted in person. The master source for on call information will be the on-call contact list located in the O&M SharePoint site

- Senior management notification will include the O&M Manager, SA Manager, and the Service Delivery Director. Escalation of a case does not remove the assignment from an individual. It is up to the manager of the group to make certain the right personnel are assigned.
- Any time a ticket is escalated, the ticket notes will be updated to reflect the escalation and the following notifications will be performed by the O&M Team:
  - Customer will receive a standard escalation notice from SN/email informing them of the escalation.
  - Person to whom case is currently assigned will be notified.
  - Manager of group to whom case is currently assigned will be notified

The Contract Manager described in Section 7 is accountable for ensuring all information is escalated to the appropriate individuals and is responsible for ensuring all contractual SLAs are documented. The Contract Manager is informed of all issue resolutions and root causes.

AWS Incident Response

AWS also provides incident response services as outlined below:

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 standards, system utilities are appropriately restricted and monitored. Below is an outline of the three-phased approach AWS has implemented to manage incidents:
Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including:

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.

Trouble ticket entered by an AWS employee

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.

Recovery Phase - the relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow - up actions and end the call engagement.

Reconstitution Phase - Once 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 the internal communication mechanisms detailed above, 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 our 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).

6.3.2. Code of Conduct (RFP 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.

Smartronix requires all employees to sign Rules of Behavior, which expressly forbids the pushing of adware, software or unauthorized marketing. Rules of Behavior also describe security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev3 security control PL-4 requires Cloud Service Providers to implement Rules of Behavior for all users. It is often the case that different Rules of Behavior apply to internal and external users. Internal users are employees of your organizations, including contractors. External users are anyone who has access to a system that you own that is not one of your employees or contractors. External users might be customers or partners, or customer prospects that have been issued demo accounts.

Smartronix Federal and Commercial (F&C) employees who have access to the Cloud Assured Managed Infrastructure as a Service [MIaaS] system (CAMS), must sign Internal Rules of Behavior. If F&C provisions accounts for customers, including management accounts, it is the F&C's responsibility to ensure that whomever F&C provisions an account to signs an External Rules of Behavior. If F&C provisions a management account to an individual customer, and then that manager in turn provisions subsequent customer accounts, it is the responsibility of the customer manager to ensure that users that he/she has provisioned sign the F&C provided Rules of Behavior. Ultimately, whoever provisions the account owns the responsibility for getting users to sign the Rules of Behavior for the accounts that they have provisioned.

AWS services are provisioned on-demand by the customer; this is the passive nature of IaaS. The customer controls how it uses its account and what content moves onto and off of its account. AWS SOC reports (available under AWS NDA) provide additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources.

6.3.3. Hosting Environment (RFP 8.3.3)

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

AWS provides capabilities that enable customers to get started quickly, with processes that are easy to repeat, through the ability to create a custom Amazon Machine Image (AMI) in Amazon Web Services. This makes sure that every developer and tester can be working with the same configuration. In addition, you can use AWS CloudFormer to take an image of your entire cloud infrastructure and create a template so you can start up exact replicas of that infrastructure for development and test.

Smartronix as a value added service provider has created dozens of application AWS CloudFormation templates that enable the rapid build-out of capabilities in a repeatable manner. There are also entire third party ecosystems providing advanced template repositories that can easily and quickly be customized.

6.3.4. Accessibility (RFP 8.3.4)

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

In 1998, The Congress of the United States of America amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. ' 794d), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.

AWS offers the Voluntary Product Accessibility Template (VPAT) upon request.

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 has incorporated Section 508 requirements and AWS has prepared a Voluntary Product Accessibility Template (VPAT) for the Console, which outlines the Console's accessibility features.

6.3.5. Application/Content Versions (RFP 8.3.5)

Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

All AWS and Smartronix external facing services are accessible using current released versions of IE, Firefox, Chrome and Safari.

6.3.6. Data Classification (RFP 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.

Smartronix has a well-defined on-boarding process that covers data classification, required security controls and compliance mandates that must be met. This includes PII, PHI, PCI, ITAR, export, and data sovereignty issues. FIPS Pub 199 addresses mechanisms for classification of data and government information systems. As part of our FedRAMP compliance we are required to document these classifications.

Our on-boarding teams are very familiar with US and Global data regulations and provide guidance and insight to our customers on the necessary security controls required and recommend best practices and compensating controls where necessary.

6.3.7. Project Schedules/Timelines (RFP 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.

Smartronix follows project planning and execution methodologies which conform to industry standard best practices, which include those of the Project Management Institute (PMI) as articulated in the Project Management Book of Knowledge (PMBOK) and instituted by our PMP certified Project Managers.

In addition, Smartronix has created and refined a detailed methodology for helping our customers rapidly adopt a cloud-centric approach to computing. This methodology, which we call FAST60 or FAST90, significantly eliminates or reduces many of the challenges of migrating to cloud adoption that are faced due the unique requirements of public sector organizations.

Specific timelines for developing, testing, and implementing solutions for customers can vary greatly, from hours to weeks or months, depending upon specific customer requirements. However, Smartronix generally delivers customer solutions in much less time than expected, and certainly in a great deal less time than traditional datacenter hardware-based approaches of the past would have allowed.

6.4. CUSTOMER SERVICE (RFP 8.4)

6.4.1. Customer Service Offering (RFP 8.4.1)

Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include:

1. Quality assurance measures;
2. Escalation plan for addressing problems and/or complaints; and
3. Service Level Agreement (SLA).

Quality Assurance Measures

Smartronix is ISO 20001:2011, ISO 9000 QMS, and CMMI Level III certified. All of our contracts follow a rigorous Quality Control and Management process to ensure timely, accurate, consistent, and cost effective delivery of services.

CMMI Level III Quality Management and Supply Chain Management ensures that any software developed or procured will be free of malicious code.

Our Quality Assurance Surveillance Processes ensure that our technical and management performance is accurately reported and that SLAs are fully documented and analyzed.

Our onboarding process for our Managed Services has successfully completed a 3PAO FedRAMP audit and meets all onboarding requirements. Post contract award Smartronix PM will ensure all staff complete all onboarding and Rules of Behavior tasks. All personnel will take Security Awareness Training and all progress towards all onboarding tasks will be reported weekly.

Smartronix will provide weekly status reports during the transition and monthly progress reports post account transition, which will include progress for the period, activities planned, status of deliverables, and any identified risks or pending SLA impacting events.

Escalation Plan for Addressing Problems and/or Complaints

The escalation process is defined at a high level in the RFP Section 6.3.1. The steps are detailed below.

All escalation process steps are performed by the O&M Team. Some of the steps may be automated.

Step	Description
➢	Ticket Queue Manager/Open by Tech: Examine all open incidents and determine actions based upon incident priority.
➢	Is this a priority 1 (high priority) incident?
➢	If it is a high priority incident, immediately notify SMX O&M Manager and SA Manager. Contact via phone with f/up email
➢	Monitor the status of the priority 1 incident providing informational updates to management at a minimum of every 30 minutes.
➢	Has the incident been resolved? If not continue to monitor.
➢	If incident is not resolved within 30 minutes, escalate ticket to next level – SA group, and notify SA manager. Update ticket notes
➢	If the incident has been resolved, notify management of the resolution. Senior management should be notified by phone during business hours.
➢	Is this a priority 2 (medium priority) incident?
➢	If so, notify the manager of the group performing the resolution. Notification should be by email.
➢	Has the incident occurred during business hours or off hours? If during business hours, notify shift manager.
➢	If the incident occurred during off hours, is the on call person available?
➢	If the on call person is not available, call the manager of the group assigned for resolution.
➢	Is the manager of the provider group available?
➢	If neither the group on-call person nor the manager of the group is available, notify senior management via email and phone.
➢	Has the time limit to resolve the incident elapsed?
➢	If the time limit to resolve has elapsed, notify the manager of the group via phone and email.
➢	Continue to monitor the incident
➢	Has the incident been resolved?
➢	If the incident has been resolved notify the customer and all personnel previously contacted of the resolution.

A critical component of success in meeting service level targets is for SMX CAMS to hold itself accountable for deviations from acceptable performance. This will be accomplished by producing standard KPI reports that can be utilized to focus on areas that need improvement. The reports will be used to identify key areas for improvement and the basis for service improvement initiatives.

A report showing all incidents related to service interruptions will be reviewed during a weekly operational review meeting. The purpose is to discover how serious the incident was, what steps are being taken to prevent reoccurrence, and if root cause needs to be pursued.

Metrics reports will be produced monthly with quarterly summaries. Metrics to be reported are:

- Total numbers of Incidents
- Number of Incidents by Severity
- Number of Incidents by Customer
- Mean time to Acknowledge – by Priority
- Mean time to Resolve - by Priority
- Percentage of incidents handled within agreed response time as define by the SLA
- Number and percentage the of incidents processed per O&M Team agent
- Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources.

SLA Management Service

Smartronix' Service Level Agreement (SLA) Management is tracked in the CloudAssured Portal. As part of the reporting process, Smartronix provides monthly status reports of ITSM-related SLAs. These SLAs include both the standard SLAs and any task-order specific SLAs included in our contract. These monthly SLA reports are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement methodology.

6.4.2. Customer Service Compliance (RFP 8.4.2)

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

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

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

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

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

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

Smartronix will identify a lead representative for each entity that executes a contract and keep that contact information current.

Smartronix' IT Service Management (ITSM) approach includes a comprehensive 24x7x365 offering using email, phone support, and the web to provide a real time communication link for our customers. All incidents and requests are cataloged in our ticketing system and ticket status change notifications are provided automatically. We provide status reports for incidents and problems through the CloudAssured Portal.

The ITSM capability is delivered through ServiceNow and enables the CloudAssured team to execute a repeatable framework for providing ITSM services. ServiceNow allows the CloudAssured service team to deploy organization-specific containers that ensure logical separation of customers' data. All customer authorized representatives, and only authorized representatives, can request service. The customer representative can submit requests, view the status of all in-progress requests, and review historical information on closed requests.

In case of regulatory or other customer driven requirements, the Smartronix CloudAssured ServiceNow implementation can restrict which types of CloudAssured team members have access to customer information. For example, all non-US Citizens or all team members who have not been screened by the customer for public trust, DoD, or other industry specific clearance process can be restricted from accessing any customer data within the ServiceNow platform.

Smartronix' CloudAssured Managed Services Solution Offering gives your organization the ability to leverage the power and scalability of the cloud while reducing the cost and complexity of managing and monitoring infrastructures and applications in-house. Our experts can provide complete management of cloud services from initial provisioning through the entire solution life-cycle. Our Managed Services span private, public, and hybrid cloud offerings, allowing your organization to focus on critical business and strategic technology efforts while leaving resource-intensive IT operations to our professional team of experts.

Smartronix' CloudAssured Managed Services manages your Infrastructure-as-as-Service (IaaS) from the networking layer through virtualization up to and including the operating systems. Our design takes a holistic view of your enterprise infrastructure and a proactive approach to identifying anomalies that may lead to incidents and could affect system performance.

Our Managed Services packages include the licensed software tools necessary for us to support your infrastructure. Although our tools are chosen by our experts to provide the best capabilities, customers may have existing tools or interoperability requirements that necessitate other selections

Smartronix also proxies direct access to AWS Support services. 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 utilize the products and features provided by AWS.

6.5. SECURITY OF INFORMATION (RFP 8.5)

6.5.1. Data protection methodology (RFP 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.

It is important that customers understand some important basics regarding data ownership and management in the cloud shared responsibility model:

- Customers continue to own their data.
- Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
- Customers can download or delete their data whenever they like.
- Customers should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

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

Data Recovery/Transfer

AWS allows customers to move data as needed on and off AWS storage using the public Internet or AWS Direct Connect (which lets customers establish a dedicated network connection between their network and AWS).

AWS Import/Export accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS transfers customer data directly onto and off of storage devices using Amazon's high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than customers upgrading their connectivity. With Import/Export encryption is mandatory, and AWS will encrypt customer data using the password they specified and transfer it onto the device.

Deleting Data

Customers can use Multi-Object Delete to delete large numbers of objects from Amazon S3. This feature allows customers to send multiple object keys in a single request to speed up their deletes. Amazon does not charge customers for using Multi-Object Delete.

Customers can use the Object Expiration feature to remove objects from their buckets after a specified number of days. With Object Expiration customers can define the expiration rules for a set of objects in their bucket through the Lifecycle Configuration policy that they apply to the bucket. Each Object Expiration rule allows customers to specify a prefix and an expiration period.

Archiving Data

With Amazon S3's lifecycle policies, customers can configure their objects to be archived to Amazon Glacier or deleted after a specific period of time. Customers can use this policy-driven automation to quickly and easily reduce storage costs as well as save time. In each rule customers can specify a prefix, a time period, a transition to Amazon Glacier, and/or an expiration. For example, customers could create a rule that archives all objects with the common prefix "logs/" 30 days from creation, and expires these objects after 365 days from creation. Customers can also create a separate rule that only expires all objects with the prefix "backups/" 90 days from creation. Lifecycle policies apply to both existing and new S3 objects, ensuring that customers can optimize storage and maximize cost savings for all current data and any new data placed in S3 without time-consuming manual data review and migration.

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.

Support Services
Smartronix works directly with our customers to manage data disposition and protection through transition. This includes management, rotation, and disposition of any Cryptographic Keys used to encrypt the data.

6.5.2. Data protection compliance (RFP 8.5.2)

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

Smartronix has a well-defined on-boarding process that covers data classification, required security controls and compliance mandates that must be met. This includes PII, PHI, PCI, ITAR, export, and data sovereignty issues. FIPS Pub 199 addresses mechanisms for classification of data and government information systems. As part of our FedRAMP compliance we are required to document these classifications.

Our on-boarding teams are very familiar with US and Global data regulations and provide guidance and insight to our customers on the necessary security controls required and recommend best practices and compensating controls where necessary.

Continuous monitoring activities ensure we are maintaining data compliance. Smartronix has developed automated monitoring scripts that ensure data is encrypted at rest and in transit. Bucket policies within the AWS S3 object storage service also enforce encryption compliance. Periodic reviews and audits of AWS CloudTrail and AWS Config logs also trigger alerts if compliance drifts occur.

6.5.3. Data Access (RFP 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.

Smartronix applies role based IAM access policies to restrict data and account access to Privileged Users. Smartronix requires all employees to sign Rules of Behavior which expressly forbids unauthorized access. Rules of Behavior also describe security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev3 security control PL-4 requires Cloud Service Providers to implement Rules of Behavior for all users. It is often the case that different Rules of Behavior apply to internal and external users. Internal users are employees of your organizations, including contractors. External users are anyone who has access to a system that you own that is not one of your employees or contractors. External users might be customers or partners, or customer prospects that have been issued demo accounts.

Smartronix Federal and Commercial (F&C) employees who have access to the Cloud Assured Managed Infrastructure as a Service [MIaaS] system (CAMS), must sign Internal Rules of Behavior. If F&C provisions accounts for customers, including management accounts, it is the F&C's responsibility to ensure that whoever F&C provisions an account to signs an External Rules of Behavior. If F&C provisions a management account to an individual customer, and then that manager in turn provisions subsequent customer accounts, it is the responsibility of the customer

manager to ensure that users that he/she has provisioned sign the F&C provided Rules of Behavior. Ultimately, whoever provisions the account owns the responsibility for getting users to sign the Rules of Behavior for the accounts that they have provisioned.

Smartronix will only use the data for purposes defined in the Master Agreement, addendums, or SLAs. Smartronix has been audited for FedRAMP compliance and ensures policies and controls are in place to prevent unauthorized use of data and information.

AWS also provides a Data Privacy policy around disclosure included below:

Disclosure of customer content: We do not disclose customer content unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure.

AWS services are provisioned on-demand by the customer; this is the passive nature of IaaS. The customer controls how it uses its account and what content moves onto and off of its account. AWS SOC reports (available under AWS NDA) provide additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources.

6.6. PRIVACY AND SECURITY (RFP 8.6)

6.6.1. NIST compliance (RFP 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.

Smartronix maintains FedRAMP accreditation for its CloudAssured Managed Services. This requires a continuous commitment to maintain NIST 800-53 Rev 4 cloud controls. We currently support all classifications of data and systems on AWS from Low to High Impact. We adhere to PII, PCI, PHI, HIPAA, HiTRUST and several other data compliance mandates for our regulated customer base. We continuously monitor and scan our environments to ensure we maintain compliance.

AWS pioneered the support for NIST 800-145 and is the industry gold standard for delivery of classic cloud services. AWS continuously innovates and provides new capabilities for managing, securing, and protecting data assets across multiple service modeles and delivery methods.

6.6.2. List of security certifications (RFP 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.

Smartronix CloudAssured Services have been certified at ISO 9001, ISO 20001, CMMI Level 3, SOC 1, SOC 2, and FedRAMP 3PAO meeting controls for NIST 800-53 rev 4.

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001
- ISO 27017
- ISO 27018
- ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) security impact levels 2 and 4
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)
- FBI Criminal Justice Information Services (CJIS)
- National Institute of Standards and Technology (NIST) 800-171
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)

For information on all of the security regulations and standards with which AWS complies, visit the AWS Compliance webpage: http://aws.amazon.com/compliance/.

6.6.3. Security Practices (RFP 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.

Advanced Security Service
Smartronix' Advanced Security (AS) Services is a customer tailored solution. Our CloudAssured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

Application Management Service
Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This

includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

Database Management Service
Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry- leading database systems. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

Log Management Service
Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core Log Aggregation service by integrating search capabilities, counters, and proactive log review analysis. The Analysis capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

Security and Regulatory Compliance Advisory Service
Smartronix' Security and Regulatory Compliance Advisor (SRCA) Service utilizes Global Intelligence for security and threat analytics to provide clients guidance in regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as they appear and evolve. Email notification is provided the day of significant threats are surfaced in industry analyses.

AWS Monitoring
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 which supports 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 as well as additional capacity protect against the possibility of DoS attacks.

The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The 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. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your 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 our 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 you. Your strict management of security groups can further mitigate the threat of port scans. If you 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, you 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. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your 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: 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 you can place your 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 you should encrypt sensitive traffic.

6.6.4. Data Confidentiality Standards (RFP 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.).

Smartronix has an identified and documented FedRAMP policy for managing Privileged Access.

This Smartronix (SMX) Cloud Assured Managed Infrastructure-as-a-Service (CAMS) Access Control and Account Management Plan details the access control and account management activities for the CAMS. It facilitates compliance with the National Institute of Standards and Technology's (NIST) Recommended Security Controls for Federal Information Systems (NIST 800-53) and the NIST Guide for Accessing the Security Controls in Federal Information Systems (NIST 800-53A). Specifically, the following NIST access controls (AC) are addressed:

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management (AM)
- AC-3 Access Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege
- IA-1 Identification and Authentication Policy and Procedures
- IA-2 Identification and Authentication (Organizational Users)
- IA-4 Identifier Management
- IA-5 Authenticator Management
- IA-6 Authenticator Feedback
- PL-4 Rules of Behavior

This plan also relates to three (3) SMX account administration procedures:

- Managing User Accounts for Major Applications
- Recertification of User Accounts and Identifying and Establishing Separation of Duties
- Maintaining Least Privilege for Users

All devices (laptops, mobile) accessing client data must use Multifactor Authentication. All managed services desktops follow a standard build and must maintain active security compliance.

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

6.6.5. Third Party Attestations (RFP 8.6.5)

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

Smartronix CloudAssured Services have been certified at ISO 9001, ISO 20001, CMMI Level 3, SOC 1, SOC 2, and FedRAMP 3PAO meeting controls for NIST 800-53 rev 4.

As mentioned above the following attestations are available for AWS:

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001
- ISO 27017
- ISO 27018
- ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) security impact levels 2 and 4
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)
- FBI Criminal Justice Information Services (CJIS)
- National Institute of Standards and Technology (NIST) 800-171
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)

6.6.6. Logging practices (RFP 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.

Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core Log Aggregation service by integrating search capabilities, counters, and proactive log review analysis. The Analysis capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

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.

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.

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.

AWS CloudTrail: Features and Benefits

Some of the many 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, see the AWS CloudTrail partners section.

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.

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.

Customer can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Customers can send thier 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 break down 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. 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.

6.6.7. Data Segmentation (RFP 8.6.7)

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

AWS provides an extremely rich set of role based access, rights management, and policy enforced access services enabling it to restrict visibility and access of data in the cloud.

AWS Identity and Access Management (IAM) is a web service that enables AWS customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With AWS IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Permissions let you specify who has access to AWS resources and which actions they can perform on those resources. Every AWS Identity and Access Management (IAM) user starts with no permissions. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user), or add the user to a group that has the desired permission.

6.6.8. Notification Process (RFP 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.

Smartronix' Incident Response (IR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' CloudAssured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The CloudAssured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

AWS has implemented various methods of external communication to support its customer base and the 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" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact. The "AWS Security Center" is available to provide you with security and compliance details about AWS. You can also subscribe to AWS Support offerings that include direct communication with the customer support team and proactive alerts to any customer impacting issues.

6.6.9. Security Controls (RFP 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.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment,

including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

6.6.10. Reference Security Architecture (RFP 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).

The following reference architecture is a typical managed architecture for our customers requiring FedRAMP level accreditation.

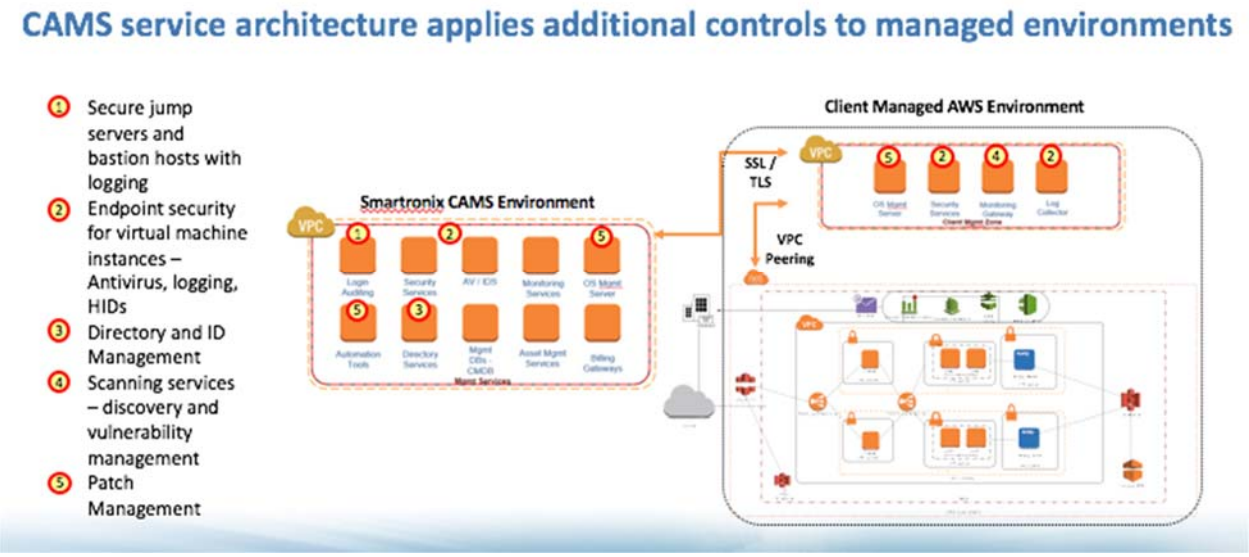


Figure 14: CAMS Security Architecture

This architecture can be customized to meet each client security and compliance mandates. Since the architecture supports receiving telemetry data from peered environments it supports SaaS, PaaS, IaaS services across multiple deployment methods including on-premises infrastructure.

6.6.11. Security Procedures (RFP 8.6.11)

(Background checks, foot printing logging, etc.) Which are in place regarding Offeror's employees who have access to sensitive data.

Smartronix maintains nearly 80% clearance of all its personnel due to the nature of its business with DoD and Federal entities. Customers can restrict access to US only and US cleared personnel if required. Smartronix also uses an advanced identity proxy service that logs all access to customer servers and is available for replay and non-repudiation services at any time. All access is also controlled by multifactor authentication support.

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 reports provides additional details regarding the controls in place for background verification.

6.6.12. Security Measures and Standards (RFP 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.

Smartronix CloudAssured Managed Services has met FedRAMP 3PAO requirements, which follows NIST 800-53 Rev 4 controls. AWS underlying IaaS also has met FedRAMP ATO.

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' CloudAssured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

Smartronix' Advanced Security (AS) Services is a custom solution. Our CloudAssured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

AWS offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift
- Flexible key management options that allow you to choose whether to have AWS manage the encryption keys or maintain complete control over your keys
- Dedicated, hardware-based cryptographic key storage options for customers to help satisfy compliance requirements

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

6.6.13. Describe policies and procedures (RFP 8.6.13)

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.

Any data breach is classified as a "Critical" impact incident and follows the complete ITIL process for Security Incident and Event Management described above.

Smartronix' Advanced Security (AS) Services is a custom solution. Our CloudAssured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

AWS Customers retain the responsibility to monitor their own environment for privacy breaches.

AWS has implemented a formal, documented incident response policy and program (including instructions on how to report internal and external security incidents). The policy addresses purpose, scope, roles, responsibilities, and management commitment. Systems within AWS are extensively instrumented to monitor key operational and security metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key metrics. When a threshold is crossed, the AWS incident response process is initiated. The Amazon Incident Response team employs industry - standard diagnostic procedures to drive resolution during business - impacting events. Staff operates 24x7x365 coverage to detect incidents and manage the impact to resolution.

AWS utilizes a three-phased approach to manage incidents:

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. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow - up actions and end the call engagement.
3. Reconstitution Phase - Once 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 the internal communication mechanisms detailed above, 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" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

AWS incident management program reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.

6.7. MIGRATION AND REDEPLOYMENT PLAN (RFP 8.7)

6.7.1. Deprovisioning (RFP 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.

Smartronix works closely with its customers in creating Sunset and Transition plans. These plans define the orderly transition of data, systems, and administrative/privileged access control.

All throughout transition and sunset Smartronix maintains responsibility for SLAs and data security.

Data portability is a key feature of the AWS offering. Multiple service exist for migrating the data and even server images rapidly and effectively across cloud boundaries.

AWS Customers have complete control over how to 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 provide that access to systems or data is restricted and monitored. In addition, customer data is 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.

6.7.2. Data Return (RFP 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.

The customer always owns the data. Smartronix can facilitate the exchange of data between the AWS environment and the Purchasing Entity using AWS provided capabilities for Import and Export or using Application provided capabilities such as database backups, log shipping, or file replication. SLAs frequently include RPO/RTO information and can be extended to other IT environments.

Alternatively, complete account ownership and management can be transitioned to another supplier.

6.8. SERVICE OR DATA RECOVERY (RFP 8.8)

6.8.1. Contingency (RFP 8.8.1)

Plans 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).

Extended downtime, unrecoverable loss, and system failures are managed using the ITIL Incident Response management framework Smartronix has put in place. Response is based on negotiated SLAs that define the criticality of the systems impacted. In general, good design and automated management completely mitigates these issues. For example, extended downtime is mitigated by minimizing single points of failure within a cloud environment. Should an entire AWS Availability go down new services can be spawned in another AZ automatically or traffic can be redirected using Load Balancers and dynamic routing. Loss of data is mitigated by automating the backup procedures to meet RPO targets. System failures can be mitigated by automating the recreation of systems using recipe based rebuilding templates.

RPO and RTO can truly be defined per application by the customer. Many of the workloads we design and deploy require 15 minute or less RTO. Treasury.gov, a site we deployed and have managed on AWS since 2010, can automatically failover between zones and regions with no downtime.

6.8.2. Methodologies (RFP 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.

Smartronix' Backup (BU) Services include system, configuration, environment and cloud services backup and restore. Backups are created and stored in the customer's cloud environment and data storage costs associated with backups are part of the customer cloud environment operating costs.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM

process, the CloudAssured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

The AWS platform enables a lightweight approach to backup and recovery due, in part, to the following characteristics:

- Computers are now virtual abstract resources instantiated via code rather than being hardware based.
- Capacity is available at incremental cost rather than up-front cost.
- Resource provisioning takes place in minutes, lending itself to real-time configuration.
- Server images are available on demand, can be maintained by an organization, and can be activated immediately.

These characteristics offer customers opportunities to recover deleted or corrupted data with less infrastructure overhead.

Protecting Configurations Rather Than Servers

The Amazon Elastic Compute Cloud (Amazon EC2) service enables the backup and recovery of a standard server, such as a web server or application server, so that customers can focus on protecting their configuration and the state of data rather than the server itself. This set of data is much smaller than the aggregate set of server data, which typically includes various application files, operating system files, temporary files, and so on. This change of approach means that regular nightly incremental or weekly full backups can take far less time and consume less storage space.

When a compute instance is started in Amazon EC2, it is based upon an Amazon Machine Image (AMI) and can also connect to existing storage volumes—for example, Amazon Elastic Block Store (Amazon EBS). In addition, when launching a new instance, it is possible to pass user data to the instance that can be accessed internally as dynamic configuration parameters.

A sample workflow is as follows:

Launch a new instance of a web server, passing it the identity of the web server and any security credentials required for initial setup. The instance is based upon a pre-built AMI that contains the operating system and relevant web server application (e.g., Apache or IIS).

Upon startup, a boot script accesses a designated and secured Amazon Simple Storage Service (Amazon S3) bucket that contains the specified configuration file(s).

The configuration file contains various instructions for setting up the server (e.g., web server parameters, locations of related servers, additional software to install, and patch updates).

The server executes the specified configuration and is ready for service. An open-source tool for performing this process called cloud-init is already installed on Amazon Linux AMIs and is also available for a number of other Linux distributions.

Figure 15 depicts a traditional backup approach and Figure 16 depicts an Amazon EC2 backup approach.

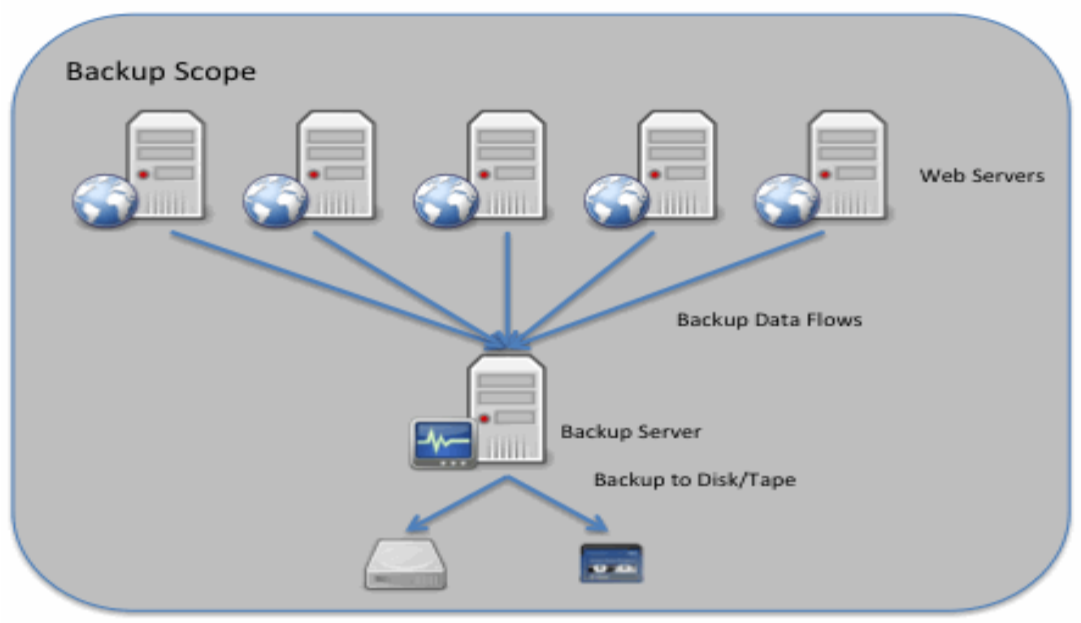


Figure 15: Traditional Backup Approach

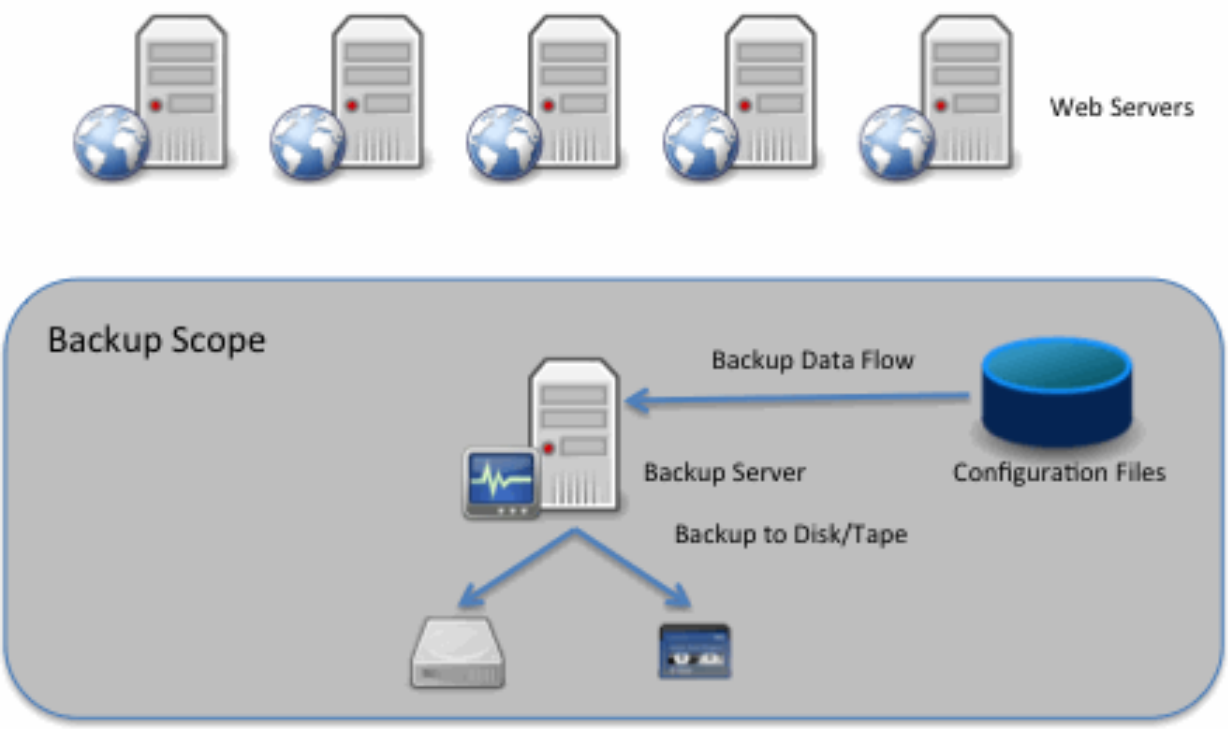


Figure 16: Amazon EC2 Backup Approach

In this case, there is no need to back up the server itself. The relevant configuration is contained in the combination of the AMI and the configuration file(s). So, the only components requiring backup and recovery are the AMI and configuration file(s).

Amazon Machine Image (AMI)
AMIs that customers register are automatically stored in their account using Amazon EBS snapshots. These snapshots reside in Amazon S3 and are highly durable. This means that the underlying storage mechanism for the AMIs is protected from multiple failure scenarios.

It is also possible to share AMIs between separate AWS accounts. Consequently, customers can create totally independent copies of the AMI by:

Sharing the original AMI to another specified AWS account controlled by the customer.

Starting a new instance based upon the shared AMI.

Creating a new AMI from that running instance.

The new AMI is then stored in the second account and is an independent copy of the original AMI. Of course, customers can also create multiple copies of the AMI within the same account.

Configuration Files
Customers use a variety of version management approaches for configuration files, and they can follow the same regime for the files used to configure their Amazon EC2 instances. For example, a customer could store different versions of configuration files in designated locations and securely control them like any other code. That customer could then back up these code repositories using the appropriate backup cycle (e.g., daily, weekly, monthly) and snapshots to protected locations. Furthermore, customers can use Amazon S3 to store their configuration files, taking advantage of the durability of the service in addition to backing up the files to an alternate location on a regular basis.

Database and File Servers
Backing up data for database and file servers differs from the web and application layers. In general, database and file servers contain larger amounts of business data (tens of GB to multiple TB) that must be retained and protected at all times. In these cases, customers can leverage efficient data movement techniques such as snapshots to create backups that are fast, reliable, and space efficient.

For databases that are built upon RAID sets of Amazon EBS volumes (and have total storage less than 1 TB), an alternative backup approach is to asynchronously replicate data to another database instance built using a single Amazon EBS volume. While the destination Amazon EBS volume will have slower performance, it is not being used for data access and can be easily snapshotted to Amazon S3 using the Amazon EBS snapshot capability.

Disaster Recovery
The AWS cloud supports many popular DR architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. With data centers in 12 regions around the world (4 in the United States), AWS provides a set of cloud-based DR services that enable rapid recovery of IT infrastructure and data.

General Disaster Recovery/COOP and Backup Requirements and Issues
Some of the minimum needs and requirements in a traditional DR approach are:

- Facilities to house additional infrastructure, including power and cooling.
- Security to ensure the physical protection of assets.

- Suitable capacity to scale the environment.
- Support for repairing, replacing, and refreshing the infrastructure.
- Contractual agreements with an Internet Service Provider (ISP) to provide Internet connectivity that can sustain bandwidth utilization for the environment under a full load.
- Network infrastructure such as firewalls, routers, switches, and load balancers.
- Enough server capacity to run all mission-critical services, including storage appliances for the supporting data, and servers to run applications and back-end services such as user authentication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), monitoring, and alerting.

AWS Capabilities for DR/COOP/Backup Solutions

With AWS, customers can eliminate the need for additional physical infrastructure, off-site data replication, and upkeep of spare capacity. AWS uses distinct and geographically diverse Availability Zones (AZs) that are engineered to be isolated from failures in other AZs. This innovative and unique AWS feature enables customers to protect applications from the failure of a single location, resulting in significant cost savings and increased agility to change and optimize resources during a DR scenario.

AWS offers the following high-level DR capabilities

Fast Performance: Fast, disk-based storage and retrieval of files.

No Tape: Eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software.

Compliance: Minimize downtime to avoid breaching Service Level Agreements (SLAs).

Elasticity: Add any amount of data, quickly. Easily expire and delete without handling media.

Security: Secure and durable cloud DR platform with industry-recognized certifications and audits.

Partners: AWS solution providers and system integration partners to help with deployments.

Solution Use Cases

AWS can enable customers to cost-effectively operate multiple DR strategies. Figure 17 shows a spectrum of scenarios—"backup & restore," "pilot light," "warm standby," and "multi-site"—arranged by how quickly a system can be available to users after a DR event.

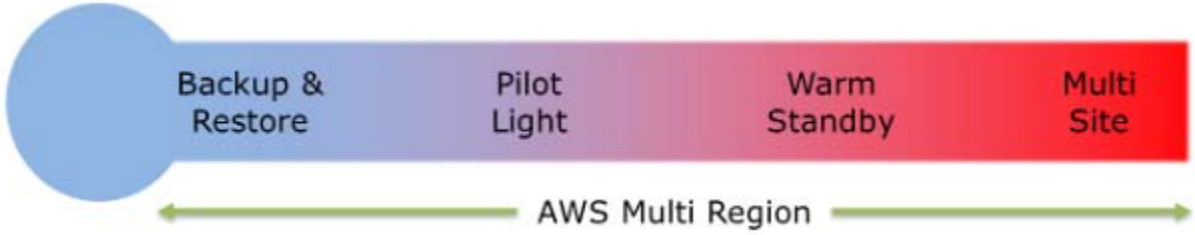


Figure 17: Spectrum of DR Options

Each DR option is discussed in more detail below:

Backup and Restore: In most traditional environments, data is backed up to tape and sent off-site regularly. Recovery time will be the longest using this method, and lack of automation leads to increased costs. Using Amazon Simple Storage Service (Amazon S3) is ideal for backup data, as it is designed to provide 99.999999999% durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. Also, with AWS Storage Gateway, customers can automatically back up on-premises data to Amazon S3.

Pilot Light for Simple Recovery into AWS Warm Standby Solution: The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small idle flame that's always on can quickly ignite the entire furnace to heat up a house as needed. This scenario is analogous to a backup and restore scenario; however, customers must ensure that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the time comes for recovery, customers would rapidly provision a full-scale production environment around the critical core.

> Amazon S3 is designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects.

Warm Standby Solution in AWS: The term "warm standby" is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. It further decreases recovery time because, in this case, some services are always running. By identifying business-critical systems, customers could fully duplicate these systems on AWS and have them always on.

Multi-Site Solution Deployed on AWS and On-Site: A multi-site solution runs in AWS as well as on a customer's existing on-premise infrastructure in an active-active configuration. During a disaster situation, an organization can simply send all traffic to AWS servers, which can scale to handle their full production load.

DR Resources

There are multiple resources to help organizations start using AWS for a DR/COOP and backup solution:

Read the AWS whitepaper Using AWS for Disaster Recovery

Read the Forrester whitepaper File Storage Costs Less in the Cloud than In-House

Review a sample AWS DR architecture

Review more information on AWS DR Capabilities and approaches

6.9. DATA PROTECTION (RFP 8.9)

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. Customers should consider the sensitivity of their data and decide if and how they will encrypt data while it is in transit and while it is at rest.

Securing Data at Rest
There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions to manual, client-side options. Choosing the right solutions depends on which AWS cloud services are being used and 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.

Additionally, the *Securing Data at Rest with Encryption* 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.

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.

The *AWS Security Best Practices* whitepaper provides greater detail on how to protect data in transit and at rest in the AWS cloud.

6.9.1. Encryption (RFP 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.

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' CloudAssured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

The following AWS services are used for encryption in transit and at rest:

- **Encrypted Data Storage** – Customers can have the data and objects they store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on

Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.

- **Dedicated, Hardware-Based Crypto Key Storage Option** – For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
- **Centralized Key Management** – For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.
- **Perfect Forward Secrecy** – For even greater communication privacy, several AWS cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.

6.9.2. Business Associate Agreements (RFP 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.

Smartronix frequently signs BAA agreements to support PHI data for its customers. AWS has a standard business associate agreement they will present to customers for signature. It takes into account the unique services AWS provides and accommodates the AWS Shared Responsibility Model.

6.9.3. Data Usage (RFP 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.

Smartronix will only use the data for purposes defined in the Master Agreement, addendums, or SLAs. Smartronix has been audited for FedRAMP compliance and ensures policies and controls are in place to prevent unauthorized use of data and information.

AWS provides a Data Privacy policy around disclosure included below:

Disclosure of customer content: We do not disclose customer content unless we are required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure.

6.10. SERVICE LEVEL AGREEMENTS (RFP 8.10)

6.10.1. SLA Applicability (RFP 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.

Smartronix provides SLAs that are completely negotiable often increasing the flow through SLAs provided by AWS.

Due to the rapidly evolving nature of AWS's product offerings, SLAs are best reviewed directly on our website:

- Amazon EC2 SLA: http://aws.amazon.com/ec2-sla/
- Amazon S3 SLA: http://aws.amazon.com/s3-sla
- Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/
- Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/
- Amazon RDS SLA: http://aws.amazon.com/rds-sla/

AWS innovates extremely quickly, and released over 700 new features or Services in 2015. The pace of innovation makes it difficult to negotiate a point-in-time SLA as new services come online daily.

AWS has over a million active Customers and AWS offers the same portfolio of self-service, highly automated web services to its Customers on a one-to-many basis. Because of this, AWS cannot commit to keep the Services or SLAs the same for certain customers but improve or change them for others. AWS needs the right to make changes across its customer base, and is not able to offer you a custom notice period.

6.10.2. Sample SLA (RFP 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.

Smartronix' core SLAs are provided below:

SLA 1: System Availability

SLA 1: "System" Availability	
Description	This SLA measures the proportion of time during the month when the "system" is fully available
Measurement	Smartronix will measure site availability by using tools that will access the site at 5 minute intervals to analyze site availability. A system is considered a series of components that make up an application or set of related applications to deliver a service. e.g. an Enterprise Resource system is made up of a web, application and database components normally deployed across multiple instances, if any of these components fully fail the "system" may be compromised.

SLA 1: "System" Availability	
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

SLA 2: Backup and Restore

SLA 2: Backup and Restoration	
Description	This SLA measures the percent of times that the platform is restored to last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restoration within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

SLA 3: Incident Response

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix' response time, per the Exceptions/Conditions in this SLA, following issue identification.
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incident receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-6pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-6pm EST M-F). Exception: Impending events; notification will happen, incident response will be initiated before follow-up notification; as clients will be previously notified (SLA 5) of the likelihood of the event.

SLA 4: Operating System Patching and Updating

SLA 4 – Operating System Patching	
Description	This SLA measures Smartronix' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied in accordance to the client planned schedule that will be defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷

SLA 4 – Operating System Patching	
	DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is considered successful when 95% of critical patches are applied to the initial environment within 10 calendar days of release from vendor and subsequent patches are applied per the customer patch schedule. Patches must be approved by customer. This will be measured on a monthly basis.
Exceptions / Conditions	Ten (10) day SLA applies to the initial environment patched. Patching of subsequent environments follow customer patch schedule. Smartronix failure to execute patching of subsequent environments per customer patch schedule shall also be considered an SLA failure for purposes of the Calculation. Any patches not approved by customer or Smartronix' CCB are excluded from the SLA Calculation.

SLA 5: Impending Event Notification

SLA 5 – Impending Event Notifications	
Description	Smartronix will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

SLA 6: Database Management Service Request

SLA 6 – Service Request – Database Management	
Description	Smartronix will initiate requested support on-demand functions for Database support made by the customer within one business day. Examples include request for database refresh from prod to Test or development, launching database instances, preforming performance analysis.
Measurement	Smartronix will measure request response based on the time requested as documented in the ITSM reporting system and the request initiation being within 1 business day.

Calculation	NUMERATOR: Number of successful request initiations within 1 business day ÷ DENOMINATOR: Number of Requests = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully initiated responses 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

SLA 7: Impending Security Threat Notification

SLA 7: Impending Security Threat Notifications	
Description	Smartronix will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new threats in the environment that may impact OS, Applications, or services used by Client.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

6.11. DATA DISPOSAL (RFP 8.11)

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

Smartronix follows NISPOM guidance for sanitization and disposal of data for services it renders.

AWS provides customers with the ability to delete their data. However, 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.

6.12. PERFORMANCE MEASURES AND REPORTING (RFP 8.12)

6.12.1. Reliability (RFP 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.

Smartronix SLA's
Smartronix will pass through in its entirety the AWS SLAs for uptime, durability, and availability of services. This includes the financially backed penalties associated with missing SLAs. AWS EC2 SLAs are backed to 99.95% uptime which exceeds your 99.5% requirement.

Service Commitments and Service Credits
Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for either Amazon EC2 or Amazon EBS (whichever was Unavailable, or both if both were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	30%

Smartronix can even extend the uptime further by providing a solution built on AWS using EC2, multiple availability zones, elastic load balancing and auto-scaling. EC2 currently provides an SLA backed uptime of 99.95% to customers. Utilizing two separate data centers (availability zones) within the same region will eliminate a single data center issue causing operational impact. Through the utilization of elastic load balancing and auto-scaling the systems, customers will be able to utilize multiple redundant servers to service users. This approach also mitigates system downtime issues allowing you to exceed the AWS SLA of 99.95% availability.

Backup Capability
AWS provides the ability to do daily incremental and weekly full snapshot capabilities. Backups are stored in S3, which provides multi-zone redundancy and eleven 9's of durability. (99.999999999%)

Backup retention periods can be set by policy to determine the length of time snapshots are kept or moved through the storage lifecycle into cold storage (archives).

6.12.2. SLA Criteria (RFP 8.12.2)

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

SLA 1: "System" Availability	
Description	This SLA measures the proportion of time during the month when the "system" is fully available
Measurement	Smartronix will measure site availability by using tools that will access the site at 5 minute intervals to analyze site availability.

SLA 1: "System" Availability	
	A system is considered a series of components that make up an application or set of related applications to deliver a service. e.g. an Enterprise Resource system is made up of a web, application and database components normally deployed across multiple instances, if any of these components fully fail the "system" may be compromised.
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

6.12.3. Support (RFP 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.

Smartronix' IT Service Management (ITSM) approach includes a comprehensive 24x7x365 offering using email, phone support, and the web to provide a real time communication link for our customers. All incidents and requests are cataloged in our ticketing system and ticket status change notifications are provided automatically. We provide status reports for incidents and problems through the CloudAssured Portal.

The ITSM capability is delivered through ServiceNow and enables the CloudAssured team to execute a repeatable framework for providing ITSM services. ServiceNow allows the CloudAssured service team to deploy organization-specific containers that ensure logical separation of customers' data. All customer authorized representatives, and only authorized representatives, can request service. The customer representative can submit requests, view the status of all in-progress requests, and review historical information on closed requests.

In case of regulatory or other customer driven requirements, the Smartronix CloudAssured ServiceNow implementation can restrict which types of CloudAssured team members have access to customer information. For example, all non-US Citizens or all team members who have not

been screened by the customer for public trust, DoD, or other industry specific clearance process can be restricted from accessing any customer data within the ServiceNow platform.

6.12.4. Incident Management (RFP 8.12.4)

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

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix' response time, per the Exceptions/Conditions in this SLA, following issue identification.
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incident receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-6pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-6pm EST M-F). Exception: Impending events; notification will happen, incident response will be initiated before follow-up notification; as clients will be previously notified (SLA 5) of the likelihood of the event.

Due to the varying nature of each workload under management, Smartronix will negotiate consequences and remedies with each Purchasing Entity for failure to meet Response and Remediation times.

6.12.5. Downtime Management (RFP 8.12.5)

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

For workloads on AWS under Smartronix management, we notify our customers of any impending service event. Smartronix will notify the customer of the possibility of an impending event or

events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.

The Smartronix Managed Patch Service team works closely with our customers to define allowable windows for downtime and can be customized to meet workload and client objectives.

AWS frequently updates and patches its services, which sometimes will cause a scheduled reboot. AWS scheduled events functionality provides greater visibility into the timing of these reboots. In addition to added visibility, in most cases you can use the scheduled events to manage reboots on your own schedule if you want to reboot before the scheduled update window. You can easily view any upcoming scheduled events for your instances in the AWS Management Console or using the API tools or command line. Reboots such as these should be infrequent, but may be necessary from time to time to apply upgrades that strengthen our security, reliability and operational performance.

There are two kinds of reboots that can be required as part of Amazon EC2 scheduled maintenance – instance reboots and system reboots. Instance reboots are reboots of your virtual instance, and are equivalent to an operating system reboot. System reboots require reboots of the underlying physical server hosting an instance. If you do not take any action, the impact on your instance is the same in both cases – during your scheduled maintenance window your instance will experience a reboot that in most cases takes a few minutes.

You also have the option to manage these reboots yourself at any time prior to the scheduled maintenance window. When you manage a reboot yourself, your instance will receive the upgrade when you reboot and your scheduled maintenance window will be cancelled (note that scheduled events can sometimes take up to 1 hour to refresh once a reboot has been completed).

6.12.6. DR Management: (RFP 8.12.6)

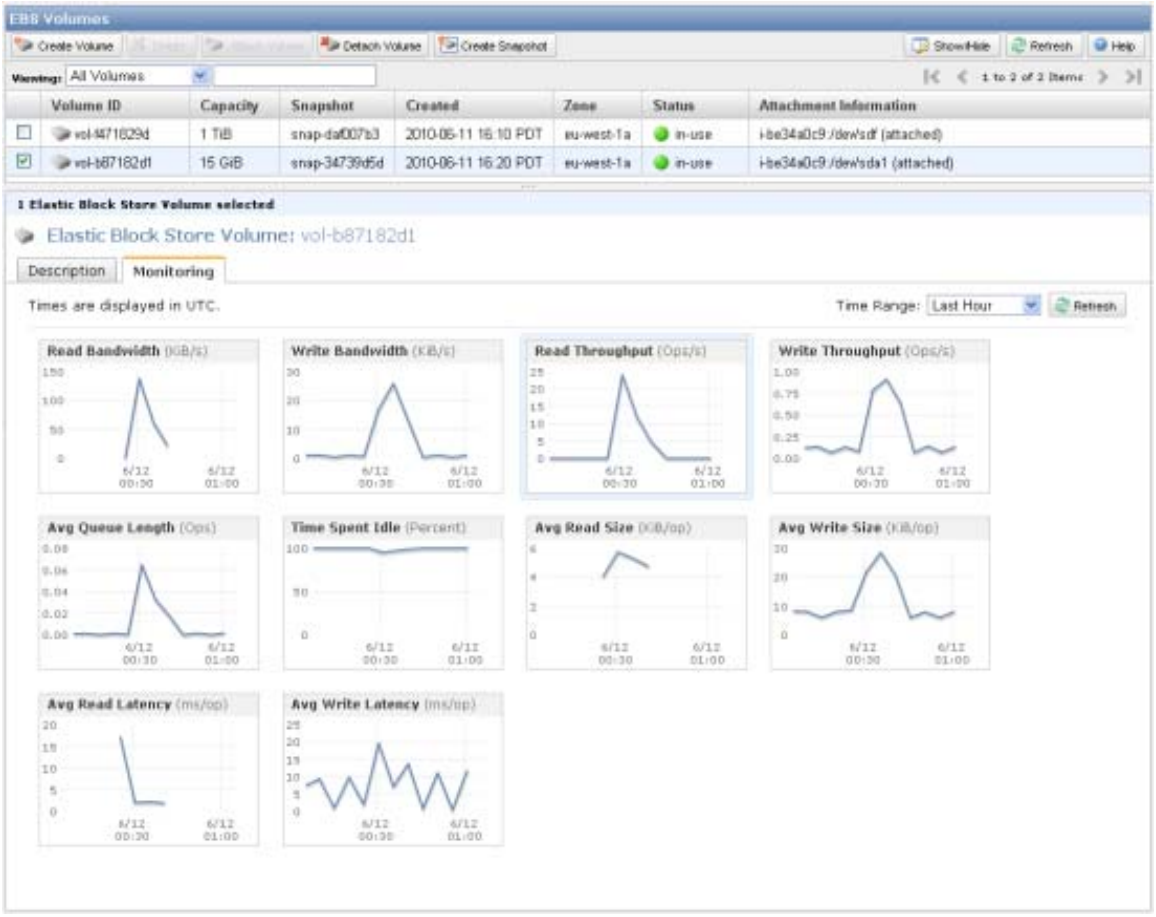
Describe the consequences/SLA remedies if disaster recovery metrics are not met.

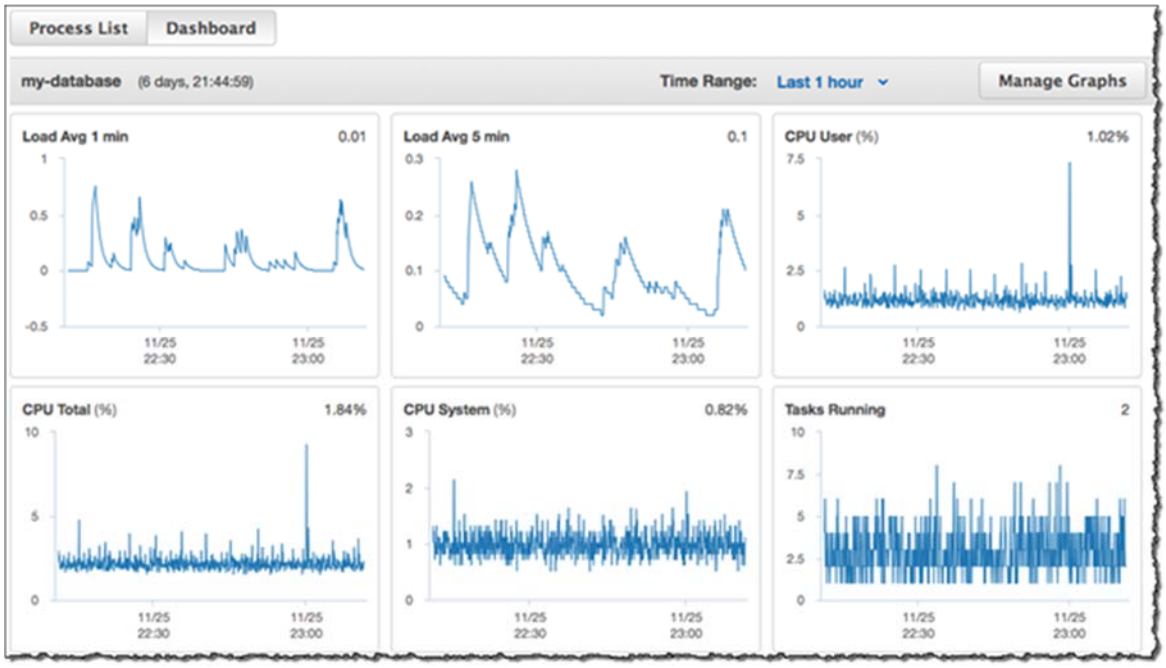
SLA remedies include discounting monthly service payments and providing service credits for the underlying infrastructure if the SLA objective is not met due to AWS availability issues. Smartronix recommends individually negotiating metrics and SLA penalties that are dependent on the criticality of the service.

6.12.7. Sample Performance Report (RFP 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.

AWS CloudWatch metrics are web accessible and contain near real time metrics measured at 1 minute intervals.





These are just a few of the dashboard views providing near real service health data.

6.12.8. Usage Reports (RFP 8.12.8)

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

Smartronix provides complete capability to print historical, statistical, and usage reports for all cloud services directly through the AWS Management Console. Additionally, Smartronix provides access to in depth customized billing reports through its CloudCheckr billing service.

The Smartronix Billing Service is designed in support of customers where Smartronix is providing AWS resale. Customers are provided a single consolidated bill of all utilized services. Additionally, the level of billing detail is flexible and may be designed to support customer requirements including chargeback purposes.

6.12.9. On-Demand Availability (RFP 8.12.9)

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

On demand deployment is available 24x365.

6.12.10. Scalability (RFP 8.12.10)

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

On demand elasticity is available 24x365.

Elastic Load Balancing and Auto Scaling can automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.

Auto Scaling

Auto Scaling allows customers to automatically scale their Amazon EC2 capacity up or down 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 cooldown 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 your 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 Figure 18.

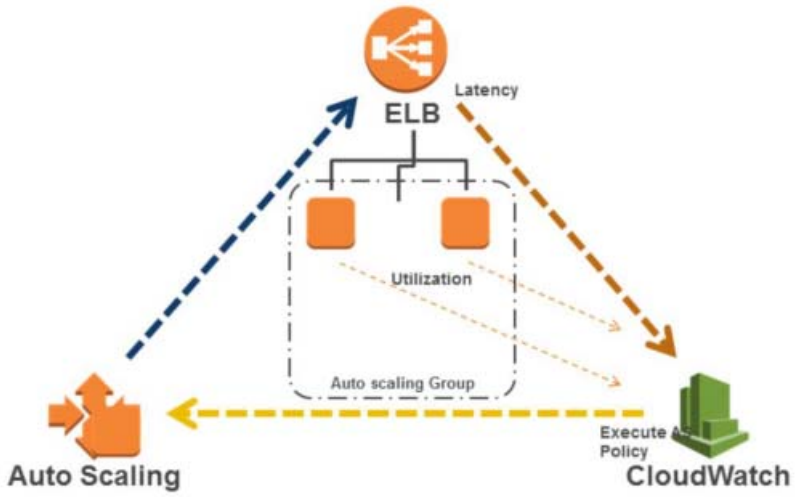


Figure 18: Auto Scaling with ELB and CloudWatch alarms

6.13. CLOUD SECURITY ALLIANCE (RFP 8.13)

Describe your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.

AWS is compliant with Level 1 CSA STAR Registry Self-Assessment. Please refer to AWS' self-assessment found within our Risk and Compliance Whitepaper, included as Attachment B of this proposal.

This is the latest CAIQ (v3) released by the CSA.

b. Completion of Exhibits 1 and 2 to Attachment B.

In our opinion, there is no response required for Exhibit B. Exhibit A questions refer to the Exhibit B for mapping references to common standards. Please refer to the completed AWS' self-assessment found within our Risk and Compliance Whitepaper, page 25-61.

This is the latest CAIQ (v3) released by the CSA.

c. Completion of a CSA STAR Attestation, Certification, or Assessment.

Per the CSA definitions, AWS aligns with Level 2 via the determinations in our third party audits for SOC and ISO:

- Level 2 Attestation is based on SOC2, which can be requested under NDA - http://aws.amazon.com/compliance/contact/
  The SOC 2 report audit attests that AWS has been validated by a third party auditor to confirm that AWS' control objectives are appropriately designed and operating effectively.
- Level 2 Certification is based on ISO 27001:2005 – the AWS ISO 27001:2005 certification is available on our website: http://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

All of the AWS self-assessed assertions within the CSA STAR Registry Self-Assessment are backed by independent, third party audits across multiple compliance programs. We continue to assert we raise the bar on CSA's "attestation" and "certification" program.

d. Completion CSA STAR Continuous Monitoring.

Per the CSA website, CSA Level 3 Continuous Monitoring is still under development. AWS has implemented and documented a Continuous Monitoring Plan which defines AWS' approach to conducting continuous monitoring with its authorizing officials within the FedRAMP Security Assessment Framework. It is based on the continuous monitoring process described in NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization, and has been reviewed and validated by a third-party assessor as part of our annual FedRAMP Assessment. It is made available to customers within the AWS FedRAMP Package which can be obtained under NDA through https://aws.amazon.com/compliance/contact/

6.14. SERVICE PROVISIONING (RFP 8.14)

6.14.1. Processes (RFP 8.14.1)

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

Smartronix created and evolved an Integrated Product Team approach for rapidly delivering services for our Department of Interior customer. The IPT consists of members of the program management office, the technology group and functional support groups. The IPT will consist of experts from both Team Smartronix and the Government, representing a fully integrated and collaborative team that is responsible for delivering core elements of the project.

This approach has worked extremely well for our DOI customers ensuring we make all deadlines for rapid delivery of cloud services. The IPT ensures all Security, Business and Technical stakeholders are aligned on objectives, requirements, and timelines. This approach has enabled us to deliver complete services to DOI within a few weeks of contract award. The IPT model is shown in the figure 19 below:

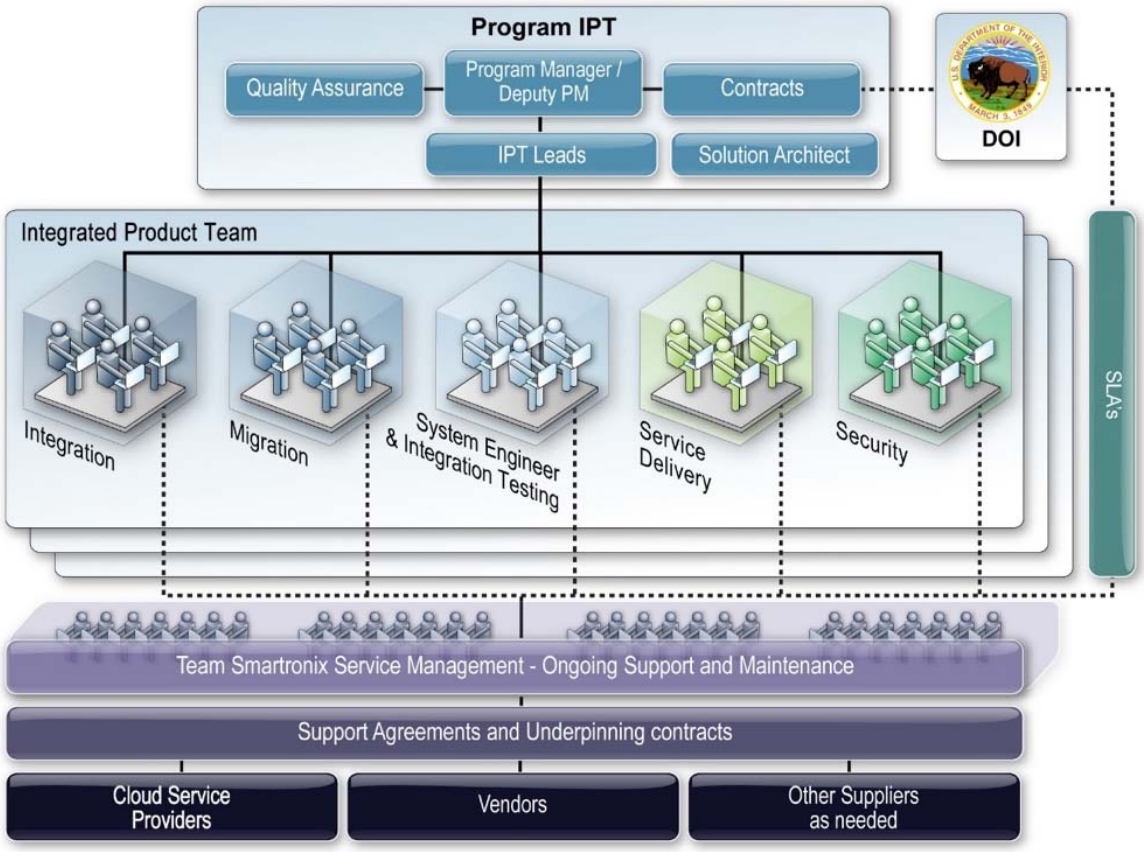


Figure 19. Smartronix DOI IPT used for FCHS Task Orders

6.14.2. Standard Lead Time (RFP 8.14.2)

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

Provisioning into an existing VPC can happen on demand via self-service. Initial provisioning of accounts and access to new environments vary from 1 day of basic administrative activities through multiple weeks depending on complexity and security requirements. Typical web based workloads utilizing a multitier architecture are deployed from start to finish in just a few weeks.

6.15. BACK UP AND DISASTER PLAN (RFP 8.15)

Amazon's infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

Availability

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 you with 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 that 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, they are each fed 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.

You should architect your 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.

Fault-Tolerant Design

Amazon's infrastructure has a high level of availability and provides you with 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 you with 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 that 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 utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed 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.

You should architect your 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 scenarios, including natural disasters or system failures. However, you 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, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), South America (Sao Paulo), and China (Beijing).

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.

6.15.1. Retention Periods (RFP 8.15.1)

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

Smartronix can apply lifecycle information policies on the customer's behalf ensuring data can move across storage tiers and if necessary into immutable storage devices for archiving. AWS policies include the ability for automatic disposition or complete lockdown meeting WORM retention requirements.

Many of Smartronix AWS customers use Amazon Glacier for long-term storage of their mission-critical data. They benefit from Glacier's durability and low cost, along with the ease with which they can integrate it in to their existing backup and archiving regimen. To use Glacier, you create vaults and populate them with archives (either directly or by using S3 lifecycle rules).

Smartronix can create a Vault Lock policy on a vault and lock it down. Once locked, the policy cannot be overwritten or deleted. Glacier will enforce the policy and will protect your records according to the controls (including a predefined retention period) specified therein.

6.15.2. DR Strategy (RFP 8.15.2)

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

Cloud services should be designed to eliminate single points of failure within the solution. Many IT teams look at the cloud as nothing but another platform to re-host services and take a simplistic "Lift and Shift" approach. This limits your High Availability options and provides practically little value. Cloud optimized designs make use of multiple Availability Zones and ensure success even if an entire AWS datacenter campus goes down. It's important to know that each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone. By architecting the solution to balance load across AZs you remove the datacenter and localized issues as points of failure. Amazon regions are also distinct and logically separated. Master control software that fails for an entire region would not affect other regions. AWS has had two incidents in the past five years that effected services across Availability Zones for our customers. None of these issues impacted regional failover and none of the issues caused any downtime for our clients that we designed their HA solutions.

Regional failover requires strategies for data synchronization. This is usually achieved at the database layer or at the publishing layer. Smartronix has several mitigation topologies that are supported by AWS to enable full-automated regional failover if required. If required, failover to alternate cloud providers or alternate physical sites is possible as well. RPO and RTO analysis require detailed understanding of the application topology and tolerance for latency based replication. This is a major reason for working with a Premier AWS Partner like Smartronix because we have the experience and expertise to design cloud topologies that are optimized for your workloads.

6.15.3. Infrastructure (RFP 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.

AWS Regions and Availability Zones: The AWS cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where we have 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 you the ability to operate production applications and databases that are more highly available, fault tolerant and scalable than would be possible from a single data center. AWS currently has 12 regions and 32 Availability Zones throughout the world: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), South America (Sao Paulo), and China (Beijing). Information on each Region can be found at http://aws.amazon.com/about-aws/global-infrastructure/.

The AWS products and services that are available in each region are listed at: http://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/.

Figure 20 depicts the current AWS regions and Edge Locations, along with new regions that are coming soon.

Figure 20: Global Map of AWS Regions and Edge Locations

Figure 21 illustrates the relationship between regions and Availability Zones.

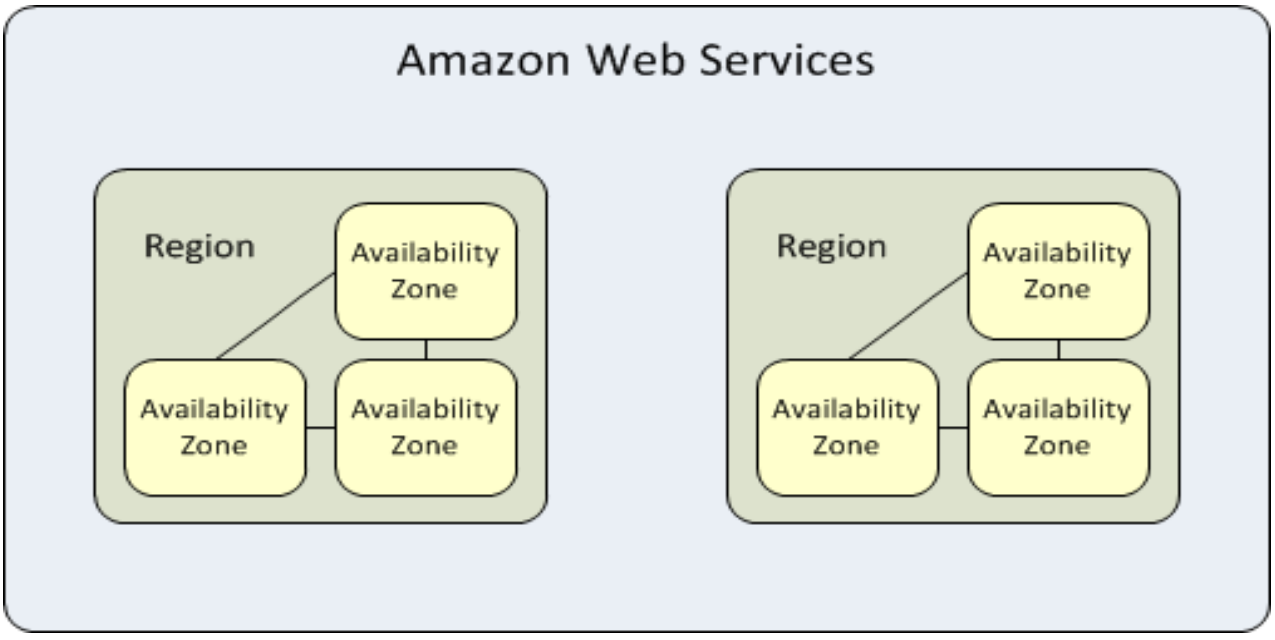


Figure 21: Regions and Availability Zones

6.16. SOLUTION ADMINISTRATION (RFP 8.16)

6.16.1. Identity Management (RFP 8.16.1)

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

Smartronix professional services team can provide identity federation and integration services to allow complete management of identity and user accounts using the existing on-premises directory services. Additionally, AWS provides services that facilitate the integration of Active Directory as well as enable isolated management of identities in the cloud.

AWS Identity and Access Management (IAM) is a web service that enables AWS customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With AWS IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Permissions let you specify who has access to AWS resources and which actions they can perform on those resources. Every AWS Identity and Access Management (IAM) user starts with no permissions. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user), or add the user to a group that has the desired permission.

This service can be provided directly to the Purchasing Entity to completely manage via self-service.

6.16.2. Anti-Virus Protection (RFP 8.16.2)

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

Smartronix' Antivirus (AV) Management Service protects your environment against malware by ensuring that the specified AV software is installed, up-to-date, and active, and is running current malware signatures. When malware is detected, we proactively ensure quarantine and automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with your AV policies.

The service is provided through a consolidated management framework. Smartronix' CloudAssured MSP offering leverages distributed relays and customer policy-based isolation to ensure the highest reasonable security. The AV functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the CloudAssured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates are applied as soon as available to enable up-to-date protection of customer systems. Customers can apply custom agent signatures through the CloudAssured ServiceNow portal.

6.16.3. Successor Data Migration (RFP 8.16.3)

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

Smartronix works directly with our customers to manage data migration through transition. This includes management, rotation, and disposition of any Cryptographic Keys used to encrypt the data.

Smartronix works closely with its customers in creating Migration and Transition plans. These plans define the orderly migration of systems and data and transition of management of data, systems, and administrative/privileged access control.

Data portability is a key feature of the AWS offering. Multiple services exist for migrating the data and server images rapidly and effectively across cloud boundaries. Examples include AWS Import/Export service and VM Import/Export services.

AWS Customers have complete control over how to 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 provide that access to systems or data is restricted and monitored. In addition, customer data is 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.

6.16.4. Solution Administration (RFP 8.16.4)

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

Smartronix currently delivers and manages cloud solutions for hundreds of customers. We have well established methodologies and processes based on ISO 20001 and ITSM best practices. Our cloud practice is structured to support a tiered help desk ranging from initial incident acknowledgement through triage and escalation to industry certified subject matter experts. This model scales very effectively and has been a proven model for large BPAs and contracts supporting multiple entities. Examples include our DoD-wide cloud contract for SPAWAR supporting dozens of entities across multiple service branches through our government wide vehicle at DOI (Foundation Cloud Hosting Services) where we actively administer solutions for HHS, DOI, National Park Service, Bureau of Ocean Engineering and Mining, and others.

Our management tools are designed to support multiple tenants while maintaining the necessary logical and physical isolation requirements. Our solution delivery team is distributed across the United States and supports clients across multiple geographies.

6.16.5. Application of Administration Policies (RFP 8.16.5)

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

Smartronix delivers and manages cloud services for a wide variety of customers, each with their own unique requirements for administration policies. Each customer can completely define their policies and Smartronix will apply those policies in the management of their solution. Smartronix

maintains configuration control items (CIs) for each entity within our ServiceNow ITSM portal. This allows us to manage unique requirements per customer. Most of our deployments use DevOps based automation in the building of the solutions. This allows us to tailor each recipe per customer and then manage the infrastructure in the same way we manage our code repositories. This approach offers the most flexibility and repeatability of service delivery to our customers.

6.17. HOSTING AND PROVISIONING (RFP 8.17)

The AWS cloud provides multiple methods for provisioning services including using existing on-premises tools for the migration of server resources across environments. The common tools used to provision AWS Services are listed below.

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. 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 lets customers provision resources across multiple regions.

Command Line Interface

The AWS Command Line Interface (CLI) is a unified tool used to manage AWS cloud services. With just one tool to download and configure, customers can control multiple AWS resources from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon Simple Storage Service (Amazon S3).

Use Existing Management Tools

Many of the tools that organizations use to manage on-premises environments can be integrated with AWS as well. Integrating an AWS environment can provide a simpler and quicker path for cloud adoption, because a customer's operations team does not need to learn new tools or develop completely new processes. For example:

AWS Management Portal for vCenter enables customers to manage their AWS resources using VMware vCenter. The portal installs as a vCenter plug-in within the existing vCenter environment. Once installed, it enables customers to migrate VMware VMs to Amazon EC2 and manage AWS resources from within vCenter. The AWS resources that customers create using the portal can be located in their AWS account, even though those resources have been created using vCenter. For experienced VMware administrators, AWS Management Portal for vCenter provides a familiar look and feel that can make it easy to start using AWS. AWS Management Portal for vCenter is available at no additional charge.

The Amazon EC2 VM Import Connector extends the capabilities of VMware vCenter to provide a familiar graphical user interface customers can use to import their preexisting Virtual Machines (VMs) to Amazon EC2. Using the connector, importing a VM is as simple as selecting a VM from the vSphere infrastructure, and specifying the AWS region, Availability Zone, operating system, instance size, security group, and Amazon Virtual Private Cloud (Amazon VPC) details (if desired) into which the VM should be imported. Once the VM has been imported, customers can launch it

as an instance from the AWS Management Console and immediately take advantage of all the features of Amazon EC2.

AWS Management Pack for Microsoft System Center enables customers to view and monitor their AWS resources directly in the Operations Manager console. This way, customers can use a single, familiar console to monitor all of their resources, whether they are on-premises or in the AWS cloud. You get a consolidated view of all AWS resources across regions and Availability Zones. It also has built-in integration with Amazon CloudWatch so that the metrics and alarms defined in Amazon CloudWatch surface as performance counters and alerts in the Operations Manager console. Information on AWS Management Pack for Microsoft System Center can be found here.

6.17.1. Provisioning Processes (RFP 8.17.1)

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

Smartronix provides several ways to enable server and service provisioning. To start, Smartronix has built a set of customizable templates that automate the account provisioning and VPC stack creation for AWS. This stack template provides a best practices approach for network, boundary, NACL, Security Group configuration, IAM policies, Subnets, and basic metered operations management. Smartronix DevOps teams also have a wide array of Chef and Jenkins based recipes for securely deploying common stacks on AWS. The standard automation stack includes Chef, Jenkins, and GitHub used in conjunction with AWS Service Catalog, AWS Cloud Formation and Command Line Interface scripts. This stack can be completely customized by each customer or the customer can choose to use the raw tools provided directly by AWS.

Smartronix works closely with our managed customers to build gold image based AMIs that meet their security and compliance standards. These images become the baseline configuration for all deployed services.

AWS OpsWorks also provides a simple and flexible way to create and manage stacks and applications. With AWS OpsWorks, you can provision AWS resources, manage their config, deploy applications to those resources, and monitor their health.

6.17.2. Tool Sets: (RFP 8.17.2) (Rob)

Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone and 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).

As mentioned in the previous section above, Smartronix and AWS provide several mechanisms for server and server stack deployment. These range from manual processes of using Console and Command Line through the ability to launch CloudFormation templates via a Service Catalog.

When a compute instance is started in Amazon EC2, it is based upon an Amazon Machine Image (AMI) and can also connect to existing storage volumes—for example, Amazon Elastic Block Store (Amazon EBS). In addition, when launching a new instance, it is possible to pass user data to the instance that can be accessed internally as dynamic configuration parameters. AMIs that customers register are automatically stored in their account using Amazon EBS snapshots. These snapshots reside in Amazon S3 and are highly durable. This means that the underlying storage mechanism for the AMIs is protected from multiple failure scenarios.

Storage provisioning is automatic as well. Through the console, CLI, or various integrated tools administrators can attach new block storage devices to instances or snapshot an existing storage device and create a new larger volume from that snapshot.

As mentioned above, you can use many of the existing tools you use today for management and monitoring of the infrastructure. Integrating an AWS environment can provide a simpler and quicker path for cloud adoption, because a customer's operations team does not need to learn new tools or develop completely new processes. These tools include AWS VMWare Management Pack for vCenter and AWS Management Pack for Microsoft System Center.

Smartronix manages several customers that use an array of hybrid tools for managing across on-premises and cloud environments. These tools include standardized patch management, antivirus management, file integrity monitoring, and SIEM based log aggregation tools. Smartronix fully supports the integration and management of these services.

As additional value added services, Smartronix has a standard management offering that customers can also use which includes Trend Micro, Splunk, ScienceLogic's EM7 and ServiceNow. These tools have been designed pure cloud deployments as well as on-premises management.

6.18. TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE) (RFP 8.18)

6.18.1. Offerings (RFP 8.18.1)

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

AWS provides several capabilities that ease the automation of the creation of testing and training environments. You can get started quickly, with processes that are easy to repeat, through the ability to create a custom Amazon Machine Image (AMI) in Amazon Web Services. This makes sure that every developer and tester can be working with the same configuration. In addition, you can use AWS CloudFormer to take an image of your entire cloud infrastructure and create a template so you can start up exact replicas of that infrastructure for development and test. https://aws.amazon.com/dev-test/

More Efficient Development Lifecycle: Production systems may be easily cloned for use as development and test environments. Staging environments may be easily promoted to production.

Improved Testability: Never run out of hardware for testing. Inject and automate testing at every stage during the development process. AWS customers can spin up an "instant test lab" with pre-configured environments only for the duration of the test.

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. It includes software

from over 2300 trusted vendors like SAP, Zend, Microsoft, IBM, Canonical, and 10gen as well as many widely used open source offerings including WordPress, Drupal, and MediaWiki.

AWS Test Drive provides a private IT sandbox environment containing preconfigured server based solutions. In under an hour, and using a step-by-step lab manual and video, launch, login and learn about popular 3rd party IT solutions, powered by AWS and CloudFormation.

Smartronix also provides demo access to its CloudAssured Services. Each client also is trained on the use of the environment.

6.18.2. Proof of Concept Environment (RFP 8.18.2)

Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Smartronix has a pre-built POC environment that showcases how we meet mandatory and enhanced requirements. This environment showcases the automated Service Catalog provisioning capabilities of AWS integrated with a FedRAMP compliant monitoring and management capability.

Typically for each customer we provide an initial set of operating capability that meets their workload requirements. This could be as simple as a development and test sandbox environment to as complicated as a multitier LAMP stack with autoscaling capabilities. These POC environments are designed to educate and engage the customers on what is possible to rapidly implement in the AWS cloud in a cost effective manner.

6.18.3. Training and Support (RFP 8.18.3)

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

AWS provides free online access to training material, best practices, and reference architectures. This includes test access via AWS Quick Start. AWS Quick Start reference deployments are free Test Drives that help you rapidly deploy fully functional software on the AWS cloud, following AWS best practices. AWS CloudFormation templates automate the deployment, and the guides describe architecture and implementation. Quick Starts are modular and customizable. You can layer additional functionality on top or modify them for your own implementations.

Smartronix also provides the training needed for accessing and interfacing with the CloudAssured ServiceNow portal.

6.19. INTEGRATION AND CUSTOMIZATION (RFP 8.19)

6.19.1. Solution Integration (RFP 8.19.1)

Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

AWS and Smartronix provide a range of integration and compatibility capabilities. The primary integration services revolve around shared services such as Identity Federation, Monitoring tools integration, database compatibility, code deployment integration, VM compatibility, and DevOps integration.

It is important to understand that the cloud environment deployed on AWS can be treated as a logical extension of your existing datacenters. Custom IP address space, Subnets, and VPN

connectivity will enable you to treat the AWS as a private connected datacenter to your infrastructure. This means services on-premises can have network level integration to services running in AWS. Your on-premises Active Directory, for instance, can be extended into AWS or federated with AWS. Your web application services can communicate with backend services residing in your datacenter over a private connection. VM's running in your VMware environment can be imported into AWS. Your Operations Management capabilities can monitor both AWS and internal infrastructure. Even your firewalls and routers can be managed across the environments with virtual appliances running in AWS.

Integration with AWS also means your cloud server infrastructure can programmatically interact with other AWS services using published APIs. This infrastructure integration layer enables autoscaling, self-healing servers, automated capacity enhancements, and highly orchestrated services.

6.19.2. Solution Customization (RFP 8.19.2)

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

This is one of the primary strengths of our service offering and what Smartronix provides as a value added cloud services intermediary. We have the ability to custom tailor AWS environments to meet the unique requirements of various Purchasing Entities. We provide the full spectrum of cloud services from pure channel resale services through complex design, deployment, migration, and operation of FedRAMP compliant workloads.

Each customer has a unique and personalized experience when interfacing with our ServiceNow portal. Incident Response, Knowledgebase Articles, Asset Management, Configuration Databases and user interface are tailored and branded for our clients.

AWS also provides the ability to completely tailor the infrastructure to meet your unique business, technical, or security requirements.

6.20. MARKETING PLAN (RFP 8.20)

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

If successfully included in the NASPO ValuePoint award, Smartronix intends to proactively contact participating entities in several ways to raise awareness of our full cloud consulting and reselling capabilities, and our alignment with NASPO ValuePoint. Smartronix will highlight for participating entities the depth of our ability to provide compliant cloud solutions in highly regulated spaces, as we are doing for many existing public sector customers. Smartronix will also educate the AWS teams on the capabilities enabled with NASPO ValuePoint, and evangelize the use of this vehicle for all applicable solicitations.

Smartronix will work to build and deliver repeatable solutions for state governments, which can assist them in providing more cost effective services to their constituents. By leveraging the full capabilities of the cloud, state governments can not only save significant taxpayer costs, but provide much better services in a much timelier manner. Smartronix is already working on these types of initiatives, and the addition of NASPO ValuePoint to our capabilities would be an important addition to our ability to support state governments.

Smartronix will create a web landing page specifically for participating entities, in order to facilitate the ease of understanding Smartronix capabilities and finding the right Smartronix points of contact.

Finally, Smartronix would be pleased to have discussions with the NASPO ValuePoint team to collaborate on additional ways help drive a successful partnership in support of state governments.

6.21. RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS (RFP 8.21)

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.

The following description lists all of our value added service capabilities for post implementation management of the infrastructure:

Services Descriptions

Monitoring and Notification Service
Smartronix' Monitoring and Notification (M&N) Service provides real time views of your entire cloud environment, including metrics on performance, usage and availability for specific components. Configurable monitoring thresholds ensure relevant performance data and events within the environment generate notifications without excessive noise.

Smartronix' customized services leverage the available Cloud Service Provider (CSP) native services Application Programmer Interfaces (APIs) to ensure events of interest trigger notifications to our support team. Typical triggers include high CPU utilization, failing or failed virtual disk volumes, unresponsive operating systems, and disk space exhaustion. Events are aggregated and alerts are automatically generated, enabling our CloudAssured Services team to proactively and rapidly mitigate potential service issues.

SLA Management Service
Smartronix' Service Level Agreement (SLA) Management is tracked in the CloudAssured Portal. As part of the reporting process, Smartronix provides monthly status reports of ITSM-related SLAs. These monthly SLA reports are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement methodology.

Incident Response Service
Smartronix' Incident Response (IR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments and infrastructure. Smartronix' CloudAssured team will support the incident response process through incident escalation, break/fix remediation of your cloud environment and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The CloudAssured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the cloud environment or guest operating systems.

Operating System Patch Management Service
Smartronix' Operating System Patch Management Service monitors the availability of and proactively applies operating system patches and updates through the use of a patch management life-cycle. Smartronix' CloudAssured team performs monthly patching of guest operating systems based on the vendor release schedule. Maintenance and patching windows are coordinated with you to ensure operations are not impacted by system patching. The patching capability is a scripted process that will trigger the guest OS to download and apply the identified guest OS patches. The applied patches are tracked through the CloudAssured MSP system to track system configuration. Critical or security related patches are quickly escalated to the customer for approval to deploy during an out of cycle maintenance window.

Customers can opt-in (patch and update) or opt-out (do not patch, do not update) individual systems via the CloudAssured portal or by contacting the CloudAssured team.

Antivirus Management Service
Smartronix' Antivirus (AV) Management Service protects your environment against malware by ensuring that the specified AV software is installed, up-to-date, and active, and is running current malware signatures. When malware is detected, we proactively ensure quarantine and automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with your AV policies.

The service is provided through a consolidated management framework. Smartronix' CloudAssured MSP offering leverages distributed relays and customer policy-based isolation to ensure the highest reasonable security. The AV functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the CloudAssured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates are applied as soon as available to enable up-to-date protection of customer systems. Customers can apply custom agent signatures through the CloudAssured ServiceNow portal.

Boundary Management Service
Smartronix' Boundary Management (BM) Service is a proactive monitoring and management service providing configuration management of cloud service provider components for networking, firewalls, virtual private networking (VPN), subnets, access control lists (ACLs), and virtual networks.

Our CloudAssured team will manage and monitor boundary protection and cloud environment network operations to ensure a secure and highly-available environment for customer data and applications. The BM service quickly identifies, mitigates, and implements network level changes in response to events or customer requests. The changes include VPN tunnel configuration, firewall policy changes to ACLs, IP route configurations, public IP allocation for service advertising, deployment of load balancing capabilities, and deployment of new cloud IP subnets.

Log Aggregation Service
Smartronix' Log Aggregation (LA) Service captures cloud service provider logs, guest OS logs, and network logs. Alerts are generated for critical events and key performance indicators within the environment, which then automatically trigger an operational response.

Using the LA Service and Smartronix' change management process, the CloudAssured team monitors the IaaS environment for possible security incidents through event filters and alerts, and performs change management of event filters implemented to ensure known critical events are identified and escalated. This service is filter-driven by a set of unwanted event types. These events include items such as cloud infrastructure configuration changes, instance termination, and excessive CPU utilization. These event filters are customized through-out the MSP term as patterns develop from lessons learned specific to the customer's applications.

Please note that log correlation, search, and analysis is not part of this service – see Security Services – Enhanced Log Aggregation and Analysis.

Backup Service
Smartronix' Backup (BU) Services include system, configuration, environment and cloud services backup and restore. Backups are created and stored in the customer's cloud environment and data storage costs associated with backups are part of the customer cloud environment operating costs.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM process, the CloudAssured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

Billing Advisory Service
Smartronix' Billing Advisory (BA) Service provides proactive usage reviews and recommendations for optimization of cloud environments to lower your cloud costs and improve performance. Recommendations incorporate our extensive experience with cloud environments, familiarity with your workloads, and our advanced tool sets' ability to model future spend as a function of utilization and various cost models offered by cloud service providers.

Infrastructure Advisory Service
Smartronix' Infrastructure Advisory (IA) Services provides prescriptive guidance on cloud services optimization, including capacity management reviews, architectural reviews and best practices reviews, auto-scaling tuning, and migration paths for on-premise workloads. These reviews leverage our CloudAssured - Well Architected guidelines and ITSM process.

The CloudAssured - Well Architected Review is a detailed analysis of your infrastructure, a thorough review of security practices, application integration architectures, and sizing of resources. This review enables Smartronix' CloudAssured team to ensure customers are leveraging cloud services in line with CSP best practices while delivering cost effective and secure service delivery.

Disaster Recovery Service
Smartronix' Disaster Recovery (DR) Service defines a DR architecture and processes to provide full planning, annual testing and execution of a managed disaster recovery solution encompassing applications, systems, and environments. Our CloudAssured team will work with you to ensure your Recovery Time Objective/Recovery Point Objective (RTO/RPO) are appropriate to your mission and to architect the solution to fulfill the requirements at the lowest cost.

Advanced Monitoring Service
Smartronix' Advanced Monitoring (AM) Service provides deeper visibility into your entire environment. Using header tags, synthetic transactions, agent based heath tools, and state-of-the-art tools, processes, and best practices, the Smartronix CloudAssured team will configure advanced monitoring to discover and optimize a comprehensive suite of availability and performance metrics.

Enhanced Data Encryption Service
Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' CloudAssured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

Advanced Security Service
Smartronix' Advanced Security (AS) Services is a custom solution. Our CloudAssured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

Application Management Service
Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

Database Management Service
Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry- leading database systems. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

Web Management and CDN Service
Smartronix' Web Management and CDN (WMC) Service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks, including the operations and management of third party CDN services. We provide proactive security monitoring of the site distribution, availability monitoring, maintenance, configuration

management, patching and security of the environment and applications. External availability and performance monitoring is also available.

DevOps and CI/CD Service
Smartronix' DevOps and CI/CD (DC) Service is a highly configurable environment and is customized to customer needs. Smartronix' CloudAssured team DevOps specialists work with your development and operations teams to provide a turnkey CI/CD environment for your organization. Recommendations, deployment, and operation of orchestration tools, code repositories, testing suites, workflow management, service deployment, and automated scaling of environments is included.

Service Desk Service
Smartronix' Service Desk provides front line (Tier 1 / Help Desk) support for end users in your organization. Smartronix' CloudAssured team user support specialists create and track issues from report to resolution, collecting and documenting circumstances, researching and recommending resolution activities, and ensuring customer satisfaction or timely escalation for prompt closure.

Security Services

Incident Response Service
Smartronix' Incident Response (IR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' CloudAssured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The CloudAssured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

Enhanced Log Aggregation and Analysis Service
Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core *Log Aggregation* service by integrating search capabilities, counters, and proactive log review analysis. The *Analysis* capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

Security and Regulatory Compliance Advisory Service
Smartronix' Security and Regulatory Compliance Advisor (SRCA) Service utilizes Global Intelligence for security and threat analytics to provide clients guidance in regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as

they appear and evolve. Email notification is provided the day of significant threats are surfaced in industry analyses.

6.22. SUPPORTING INFRASTRUCTURE (RFP 8.22)

6.22.1. Infrastructure Requirements: (RFP 8.22.1)

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

No infrastructure is required to support any of our solutions as everything is provided via AWS. Entities can choose to use hardware based VPN services and on-premises Storage Gateway services if desired but this is not required. Additionally, customers may choose to have a AWS DirectConnect physical circuit between their environment and AWS.

6.22.2. Installation requirements: (RFP 8.22.2)

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

New Infrastructure services are provisioned on available capacity within AWS. Installation of the resource pool of cloud services is the responsibility of AWS and no costs are incurred by the customer.

6.23. ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE (RFP 8.23)

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Smartronix built its cloud service practice directly on the processes and models defined in the original NIST Cloud Reference Architectures Special Publication 500-292 from 2011.

AWS services as described above fully align with the IaaS, PaaS, and IaaS service models. In the NIST Reference Architecture, Smartronix acts as the Cloud Service Broker, and acts as the intermediary for Cloud Service Management, Orchestration, Deployment, Security, Auditing and Business Support. AWS provides the building blocks and service primitives for the underlying infrastructure. Smartronix provides the ancillary services for securely designing, deploying, managing, and operating efficiently in the cloud.

7. CONFIDENTIAL, PROTECTED AND PROPRIETARY INFORMATION

The Government Records Access and Management Act (GRAMA), UCA § 63G-2-305, provides in part that: the following records are protected if properly classified by a government entity:

(1) trade secrets as defined in Section 13-24-2, the Utah Uniform Trade Secrets Act, if the person submitting the trade secret has provided the governmental entity with the information specified in UCA § 63G-2-309 (Business Confidentiality Claims);

(2) Commercial information or non-individual financial information obtained from a person if:

(a) Disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future;

(b) The person submitting the information has a greater interest in prohibiting access than the public in obtaining access; and

(c) The person submitting the information has provided the governmental entity with the information specified in UCA § 63G-2-309;

* * * * *

(6) Records, the disclosure of which would impair governmental procurement proceedings or give an unfair advantage to any person proposing to enter into a contract or agreement with a governmental entity, except, subject to Subsections (1) and (2), that this Subsection (6) does not restrict the right of a person to have access to, after the contract or grant has been awarded and signed by all parties, ... Pricing may not be classified as confidential or protected and will be considered public information after award of the contract. Process for Requesting Non-Disclosure: Any Offeror requesting that a record be protected shall include with the proposal a Claim of Business Confidentiality. To protect information under a Claim of Business Confidentiality, the Offeror must complete the Claim of Business Confidentiality form with the following information:

1. Provide a written Claim of Business Confidentiality at the time the information (proposal) is provided to the state, and

2. Include a concise statement of reasons supporting the claim of business confidentiality (UCA § 63G-2-309(1)).

3. Submit an electronic "redacted" (excluding protected information) copy of the record. The redacted copy must clearly be marked "Redacted Version." The Claim of Business Confidentiality Form may be accessed at: http://www.purchasing.utah.gov/contract/documents/confidentialityclaimform.doc An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY", and if so identified, shall be considered non-responsive unless the Offeror removes the designation. Redacted Copy: If an Offeror submits a proposal that contains information claimed to be business confidential or protected information, the Offeror must submit two separate proposals: one redacted version for public release, with all protected business confidential information either blacked-out or removed, clearly marked as "Redacted Version"; and one nonredacted version for evaluation purposes, clearly marked as "Protected Business Confidential." The Lead State and NASPO ValuePoint are not liable or responsible for the disclosure of any confidential or proprietary information if the Offeror fails to follow the instructions of this section.

There was no Confidential, Protected or Proprietary Information provided in this response

8. EXCEPTIONS AND/OR ADDITIONS TO THE STANDARD TERMS AND CONDITIONS

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations. If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

Smartronix takes exceptions to the standard terms and conditions

9. COST PROPOSAL

Smartronix submitted the Cost Proposal via the BidSync website.

10. ATTACHMENTS

10.1. ATTACHMENT I – AWS RISK AND COMPLIANCE WHITEPAPER

Please refer to the included Attachment I – AWS Risks and Compliance Whitepaper, which has been uploaded via the BidSync website with our submission.

Amazon Web Services: Risk and Compliance

January 2016

(Consult http://aws.amazon.com/compliance/aws-whitepapers/

for the latest version of this paper)

This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance questions.

Table of Contents

Risk and Compliance Overview

AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS' part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:

- Obtaining industry certifications and independent third-party attestations described in this document
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

For a more detailed description of AWS security please see:
AWS Security Center: https://aws.amazon.com/security/

For a more detailed description of AWS Compliance please see
AWS Compliance page: https://aws.amazon.com/compliance/

Additionally, The AWS Overview of Security Processes Whitepaper covers AWS' general security controls and service-specific security.

Shared Responsibility Environment

Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the

services they choose as their responsibilities vary depending on the services used, the integration of those

services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them (described in the AWS Certifications and Third-party Attestations section of this document) to perform their control evaluation and verification procedures as required.

The next section provides an approach on how AWS customers can evaluate and validate their distributed control environment effectively.

Strong Compliance Governance

As always, AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help companies gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

Evaluating and Integrating AWS Controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This documentation assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated. This information also assists customers in their efforts to account for and to validate that controls in their extended IT environment are operating effectively.

Traditionally, the design and operating effectiveness of control objectives and controls are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation/verification, by the customer or customer's external auditor, is generally performed to validate controls. In the case where

service providers, such as AWS, are used, companies request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objective and controls. As a result, although customer's key controls may be managed by AWS, the control environment can still be a unified framework where all controls are accounted for and are verified as operating effectively. Third-party attestations and certifications of AWS can not only provide a higher level of validation of the control environment, but may relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS cloud.

AWS IT Control Information

AWS provides IT control information to customers in the following two ways:

1. **Specific control definition.** AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment. AWS' controls can be considered designed and operating effectively for many compliance purposes, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies (e.g., ISO 27001 auditors may request a SOC 1 Type II report in order to complete their evaluations for customers).

Other specific control activities relate to AWS' Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. As discussed below, AWS is compliant with FISMA Moderate standards and with the PCI Data Security Standard. These PCI and FISMA standards are very prescriptive and require independent validation that AWS adheres to the published standard.

2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, evaluation of AWS' industry certifications may be performed. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to companies that handle credit card information. With AWS' compliance with the FISMA standards, AWS complies with a wide range of specific controls required by US government agencies. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

AWS Global Regions

Data centers are built in clusters in various global regions. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Seoul) Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo).

AWS Risk and Compliance Program

AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

Risk Management

AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

In addition, the AWS control environment is subject to various internal and external risk assessments. AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.

Control Environment

AWS manages a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS' service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS' control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures.

Information Security

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

AWS Certifications, Programs, Reports, and Third-Party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

CJIS

AWS complies with the FBI's Criminal Justice Information Services (CJIS) standard. We sign CJIS security agreements with our customers, including allowing or performing any required employee background checks according to the **CJIS Security Policy**.

Law enforcement customers (and partners who manage CJI) are taking advantage of AWS services to improve the security and protection of CJI data, using the advanced security services and features of AWS, such as activity logging (**AWS CloudTrail**), encryption of data in motion and at rest (S3's Server-Side Encryption with the option to bring your own key), comprehensive key management and protection (AWS **Key Management Service** and **CloudHSM**), and integrated permission management (IAM federated identity management, multi-factor authentication).

AWS has created a Criminal Justice Information Services (CJIS) **Workbook** in a security plan template format aligned to the CJIS Policy Areas. Additionally, a CJIS Whitepaper has been developed to help guide customers in their journey to cloud adoption.

Visit the CJIS Hub Page**: https://aws.amazon.com/compliance/cjis/**

CSA

In 2011, the Cloud Security Alliance (CSA) launched **STAR**, an initiative to encourage transparency of security practices within cloud providers. The **CSA Security, Trust & Assurance Registry** (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. **AWS is a CSA STAR registrant** and has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and

document what security controls exist in AWS' Infrastructure as a Service offerings. The CAIQ provides 298 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

See: **Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1**

Cyber Essentials Plus

Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks.

It demonstrates the baseline controls AWS implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "**10 Steps to Cyber Security**". It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organizations that offer incentives for businesses holding this certification.

Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to EU (Ireland) region.

DoD SRG Levels 2 and 4

The Department of Defense (DoD) Cloud Security Model (SRG) provides a formalized assessment and authorization process for cloud service providers (CSPs) to gain a DoD Provisional Authorization, which can subsequently be leveraged by DoD customers. A Provisional Authorization under the SRG provides a reusable certification that attests to our compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation on AWS. AWS currently holds provisional authorizations at Levels 2 and 4 of the SRG.

Additional information of the security control baselines defined for **Levels 2, 4, 5, and 6 can be found at: http://iase.disa.mil/cloud_security/Pages/index.aspx**.

Visit the DoD Hub Page**: https://aws.amazon.com/compliance/dod/**

FedRAMP SM

AWS is a Federal Risk and Authorization Management Program (FedRAMPsm) Compliant Cloud Service Provider. AWS has completed the testing performed by a FedRAMPsm accredited Third-Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMPsm requirements at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMPsm repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment. The two FedRAMPsm Agency ATOs encompass all U.S. . regions (the AWS GovCloud (US) region and the AWS US East/West regions).

The following services are in the accreditation boundary for the regions stated above:

- Amazon Redshift. Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools.
- Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.
- Amazon Simple Storage Service (S3). Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.
- Amazon Virtual Private Cloud (VPC). Amazon VPC provides the ability for you to provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define.
- Amazon Elastic Block Store (EBS). Amazon EBS provides highly available, highly reliable, predictable storage volumes that can be attached to a running Amazon EC2 instance and exposed as a device within the instance.
- AWS Identity and Access Management (IAM). IAM enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

For more information on AWS FedRAMP[sm] compliance please see the AWS FedRAMP[sm] FAQs at:
https://aws.amazon.com/compliance/fedramp/

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18, or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

AWS enables covered entities and their business associates subject to FERPA to leverage the secure AWS environment to process, maintain, and store protected education information.

AWS also offers a **FERPA-focused whitepaper** for customers interested in learning more about how they can leverage AWS for the processing and storage of educational data.

The "**FERPA Compliance on AWS Whitepaper**" outlines how companies can use AWS to process systems that facilitate FERPA compliance:
https://do.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, SSL terminations in **AWS GovCloud (US)** operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the **AWS GovCloud (US) environment**.

FISMA and DIACAP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (**FISMA**). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (**DIACAP**).

GxP

GxP is an acronym that refers to the regulations and guidelines applicable to life sciences organizations that make food and medical products such as drugs, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers and to ensure the integrity of data used to make product-related safety decisions.

AWS offers a **GxP whitepaper** which details a comprehensive approach for using AWS for GxP systems. This whitepaper provides guidance for using **AWS Products in the context of GxP** and the content has been developed in conjunction with AWS pharmaceutical and medical device customers, as well as software partners, who are currently using AWS Products in their validated GxP systems.

For more information on the GxP on AWS **please contact AWS Sales and Business Development**.

For additional information please see our GxP Compliance FAQs:
https://aws.amazon.com/compliance/gxp-part-11-annex-11/

HIPAA

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information and AWS will be signing business associate agreements with such customers. AWS also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of health information. The Architecting for HIPAA Security and Compliance on Amazon Web Services whitepaper outlines how companies can use AWS to process systems that facilitate HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) compliance.

Customers may use any AWS service in an account designated as a HIPAA account, but they should only process, store and transmit PHI in the HIPAA-eligible services defined in the BAA. There are nine HIPAA-eligible services today, including:

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) using only MySQL and Oracle engines
- Amazon Simple Storage Service (S3)

AWS follows a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the security, control, and administrative processes required under HIPAA. Using these services to store and process PHI allows our customers and AWS to address the HIPAA requirements applicable to our utility-based operating model. AWS prioritizes and adds new eligible services based on customer demand.

For additional information please see our HIPAA Compliance FAQs:
https://aws.amazon.com/compliance/hipaa-compliance/

Architecting for HIPAA Security and Compliance on Amazon Web Services:
https://do.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf

IRAP

The Information Security Registered Assessors Program (IRAP) enables Australian government customers to validate that appropriate controls are in place and determine the appropriate responsibility model for addressing the needs of the Australian Signals Directorate (ASD) Information Security Manual (ISM).

Amazon Web Services **has completed an independent assessmen**t that has determined all applicable ISM controls are in place relating to the processing, storage and transmission of Unclassified (DLM) for the AWS Sydney Region.

IRAP Compliance FAQs:
https://aws.amazon.com/compliance/irap/

For more information see: **Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations**

ISO 9001

AWS has achieved ISO 9001 certification, AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.
The ISO 9001 certification covers the quality management system over a specified scope of AWS services and Regions of operations (below) and services including:

- AWS CloudFormation
- AWS Cloud Hardware Security Model (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)

- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- The underlying physical infrastructure and the AWS Management Environment

AWS' ISO 9001 accreditation covers AWS Regions including US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), South America (Sao Paulo), EU (Ireland), EU (Frankfurt) and Asia Pacific (Singapore), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

ISO 9001:2008 is a global standard for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

The AWS ISO 9001 certification can be downloaded at:
https://do.awsstatic.com/certifications/iso_9001_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 9001 certification at:
https://aws.amazon.com/compliance/iso-9001-faqs/

ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- The underlying physical infrastructure (including GovCloud) and the AWS Management Environment

ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing significant information regarding our security controls and practices.

AWS' ISO 27001 accreditation covers AWS Regions including US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), South America (Sao Paulo), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

The AWS ISO 27001 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27001 certification at:
https://aws.amazon.com/compliance/iso-27001-faqs/

ISO 27017

ISO 27017 is the newest code of practice released by the International Organization for Standardization (ISO). It provides implementation guidance on information security controls that specifically relate to cloud services.

AWS has achieved ISO 27017 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

The AWS ISO 27017 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27017_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27017 certification at:
https://aws.amazon.com/compliance/iso-27017-faqs/

ISO 27018

ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

AWS has achieved ISO 27018 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

The AWS ISO 27018 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27018_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27018 certification at:
https://aws.amazon.com/compliance/iso-27018-faqs/

ITAR

The **AWS GovCloud (US)** region supports US International Traffic in Arms Regulations (**ITAR**) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to the US. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party to validate the proper controls are in place to support customer export compliance programs for this requirement.

MPAA

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a "certification," media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS.

See the AWS Compliance MPAA hub page for additional details:
https://aws.amazon.com/compliance/mpaa/

MTCS Tier 3 Certification

The **Multi-Tier Cloud Security (MTCS)** is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The certification assessment requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

View the MTCS Hub Page at:
https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/

NIST

In June 2015 The National Institute of Standards and Technology (NIST) released guidelines **800-171,** "Final Guidelines for Protecting Sensitive Government Information Held by Contractors". This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on nonfederal systems.

AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which AWS has already been audited under the FedRAMP program. The FedRAMP Moderate security control baseline is more rigorous than the recommended requirements established in Chapter 3 of 800-171, and includes a significant number of security controls above and beyond those required of FISMA Moderate systems that

protect CUI data. A detailed mapping is available in the **NIST Special Publication 800-171**, starting on page D2 (which is page 37 in the PDF).

PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers. The AWS PCI Compliance Package includes the AWS PCI Attestation of Compliance (AoC), which shows that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 3.1, and the AWS PCI Responsibility Summary, which explains how compliance responsibilities are shared between AWS and our customers in the cloud.

The following services are in scope for PCI DSS Level 1:

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)
- The underlying physical infrastructure (including GovCloud) and the AWS Management Environment

The latest scope of services and regions for the AWS PCI DSS Level 1 certification can be found at: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

SOC 1/ISAE 3402

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with American Institute of Certified Public Accountants (AICPA): AT 801

(formerly SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This report is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

Objective Area	Objective Description
Security Organization	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
Employee User Access	Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.
Logical Security	Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
Secure Data Handling	Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.
Physical Security and Environmental Protection	Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.
Change Management	Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.
Data Integrity, Availability and Redundancy	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.
Incident Handling	Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved.

The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS' customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS' commitment to the SOC 1 report is ongoing, and AWS will continue the process of periodic audits. The SOC 1 report scope covers:

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail

- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- Amazon Workspaces

SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security and availability principles set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data. The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

SOC 3

AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically-available summary of the AWS SOC 2 report. The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process to request a SOC 2 report. The SOC 3 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services. View the AWS SOC 3 report here.

Key Compliance Questions and AWS

This section addresses generic cloud computing compliance questions specifically for AWS. These common compliance questions listed may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.

Ref	Cloud Computing Question	AWS Information
1	Control ownership. Who owns which controls for cloud-deployed infrastructure?	For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report.
2	Auditing IT. How can auditing of the cloud provider be accomplished?	Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.
3	Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment?	If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS' physical controls, they can reference the AWS SOC 1 Type II report which details the controls that AWS provides.
4	HIPAA compliance. Is it possible to meet HIPAA compliance requirements while deployed in the cloud provider environment?	HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers can use AWS services to maintain a security level that is equivalent or greater than those required to protect electronic health records. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic.
5	GLBA compliance. Is it possible to meet GLBA certification requirements while deployed in the cloud provider environment?	Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions, and build GLBA-compliant applications on AWS infrastructure. If the customer requires specific assurance that physical security controls are operating effectively, they can reference the AWS SOC 1 Type II report as relevant.

Ref	Cloud Computing Question	AWS Information
6	Federal regulation compliance. Is it possible for a US Government agency to be compliant with security and privacy regulations while deployed in the cloud provider environment?	US Federal agencies can be compliant under a number of compliance standards, including the Federal Information Security Management Act (FISMA) of 2002, Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Processing Standard (FIPS) Publication 140-2, and the International Traffic in Arms Regulations (ITAR). Compliance with other laws and statutes may also be accommodated depending on the requirements set forth in the applicable legislation.
7	Data location. Where does customer data reside?	AWS customers designate in which physical region their data and their servers will be located. Data replication for S3 data objects is done within the regional cluster in which the data is stored and is not replicated to other data center clusters in other regions. AWS customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo).
8	E-Discovery. Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements?	AWS provides infrastructure, and customers manage everything else, including the operating system, the network configuration, and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
9	Data center tours. Are data center tours by customers allowed by the cloud provider?	No. Due to the fact that our data centers host multiple customers, AWS does not allow data center tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data center physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FedRAMP℠ testing programs.
10	Third-party access. Are third parties allowed access to the cloud provider data centers?	AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS data center manager per the AWS access policy. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls.

Ref	Cloud Computing Question	AWS Information
11	Privileged actions. Are privileged actions monitored and controlled?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data is 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, ITAR, and FedRAMPsm audits.
12	Insider access. Does the cloud provider address the threat of inappropriate insider access to customer data and applications?	AWS provides specific SOC 1 controls to address the threat of inappropriate insider access, and the public certification and compliance initiatives covered in this document address insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
13	Multi-tenancy. Is customer segregation implemented securely?	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 3.1 published in April 2015. Note that AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating your Amazon EC2 compute instances at the hardware level.
14	Hypervisor vulnerabilities. Has the cloud provider addressed known hypervisor vulnerabilities?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper for more information on the Xen hypervisor and instance isolation.
15	Vulnerability management. Are systems patched appropriately?	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems.
16	Encryption. Do the provided services support encryption?	Yes. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB, and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Refer to the AWS Security white paper for more information.

Ref	Cloud Computing Question	AWS Information
17	Data ownership. What are the cloud provider's rights over customer data?	AWS customers retain control and ownership of their data. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.
18	Data isolation. Does the cloud provider adequately isolate customer data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Amazon S3 provides advanced data access controls. Please see the AWS security whitepaper for more information about specific data services' security.
19	Composite services. Does the cloud provider layer its service with other providers' cloud services?	AWS does not leverage any third-party cloud providers to deliver AWS services to customers.
20	Physical and environmental controls. Are these controls operated by the cloud provider specified?	Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FedRAMP[sm] require best practice physical and environmental controls.
21	Client-side protection. Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices?	Yes. AWS allows customers to manage client and mobile applications to their own requirements.
22	Server security. Does the cloud provider allow customers to secure their virtual servers?	Yes. AWS allows customers to implement their own security architecture. See the AWS security whitepaper for more details on server and network security.
23	Identity and Access Management. Does the service include IAM capabilities?	AWS has a suite of identity and access management offerings, allowing customers to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way. Please see the AWS web site for more information.
24	Scheduled maintenance outages. Does the provider specify when systems will be brought down for maintenance?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
25	Capability to scale. Does the provider allow customers to scale beyond the original agreement?	The AWS cloud is distributed, highly secure and resilient, giving customers massive scale potential. Customers may scale up or down, paying for only what they use.
26	Service availability. Does the provider commit to a high level of availability?	AWS does commit to high levels of availability in its service level agreements (SLA). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.9%. Service credits are provided in the case these availability metrics are not met.

Ref	Cloud Computing Question	AWS Information
27	Distributed Denial Of Service (DDoS) attacks. How does the provider protect their service against DDoS attacks?	The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks.
28	Data portability. Can the data stored with a service provider be exported by customer request?	AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport.
29	Service provider business continuity. Does the service provider operate a business continuity program?	AWS does operate a business continuity program. Detailed information is provided in the AWS Security Whitepaper.
30	Customer business continuity. Does the service provider allow customers to implement a business continuity plan?	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures.
31	Data durability. Does the service specify data durability?	Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
32	Backups. Does the service provide backups to tapes?	AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS web site.
33	Price increases. Will the service provider raise prices unexpectedly?	AWS has a history of frequently reducing prices as the cost to provide these services reduces over time. AWS has reduced prices consistently over the past several years.
34	Sustainability. Does the service provider company have long term sustainability potential?	AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high long term sustainability potential.

AWS Contact

Customers can request the reports and certifications produced by our third-party auditors or can request more information about AWS Compliance by contacting AWS Sales and Business Development. The representative will route customers to the proper team depending on nature of the inquiry. For additional information on AWS Compliance, see the AWS Compliance site or send questions directly to awscompliance@amazon.com.

Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1

The Cloud Security Alliance (CSA) is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing." [Reference https://cloudsecurityalliance.org/about/] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security *Application Security*	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. AWS has in place procedures to manage new development of resources. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	AWS Customers retain responsibility to ensure their usage of AWS is in compliance with applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/compliance) and providing certifications, reports and other relevant documentation directly to AWS Customers.
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	
Application & Interface Security *Data Integrity*	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	AWS data integrity controls as described in AWS SOC reports illustrates the data integrity controls maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 14 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	AWS Data Security Architecture was designed to incorporate industry leading practices. Refer to AWS Certifications, reports and whitepapers for additional details on the various leading practices that AWS adheres to (available at http://aws.amazon.com/compliance).
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third-party attestations and provides certain certifications, reports and other relevant documentation directly to AWS Customers.
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. The AWS ISO 27001 certification can be downloaded here: http://do.awsstatic.com/certifications/iso_27001_global_certification.pdf. The AWS SOC 3 report can be downloaded here: https://do.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external audits and risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 and Glacier services are designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website.
	AAC-03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
	AAC-03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	AWS monitors relevant legal and regulatory requirements. Refer to ISO 27001 standard Annex 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Cloud Security whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	AWS Customers designate in which physical region their data and servers will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. AWS SOC reports provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing.
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security/. Refer to ISO 27001 Appendix A Domain 12.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience *Equipment Location*	BCR -06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR -07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR - 07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
	BCR - 07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	BCR - 07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	
	BCR -07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR -08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Cloud Security Whitepaper - available at http://aws.amazon.com/security.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR -09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	AWS CloudWatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	BCR - 09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
	BCR - 09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	
Business Continuity Management & Operational Resilience *Policy*	BCR -10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR -11.1	Do you have technical control capabilities to enforce tenant data retention policies?	AWS provide customers with the ability to delete their data. However, AWS Customers retain control and ownership of their data so it is the customer's responsibility to manage data retention to their own requirements. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. For additional information refer to https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR -11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	
	BCR -11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	AWS backup and redundancy mechanisms have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 12 and the AWS SOC 2 report for additional information on AWS backup and redundancy mechanisms.
	BCR -11.5	Do you test your backup or redundancy mechanisms at least annually?	
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Whether a customer is new to AWS or an advanced user, useful information about the services, ranging from introductions to advanced features, can be found on the AWS Documentation section of our website at https://aws.amazon.com/documentation/.
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	AWS maintains an ISO 9001 certification. This is an independent validation of AWS quality system and determined that AWS activities comply with ISO 9001 requirements. AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to aws.amazon.com/security/security-bulletins/. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS system development lifecycle (SDLC) incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. In addition, refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	AWS' program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management *Production Changes*	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?	AWS SOC reports provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 12 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user-friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console has also supports tagging.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region and South America (Sao Paulo).
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	AWS Customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region and South America (Sao Paulo).
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	All of the AWS APIs are available via SSH-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Customers may also use third-party encryption technologies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	AWS Customers retain control and ownership of their own data. Refer to the AWS Customer Agreement for additional information.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	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. If a hardware device is unable to be

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).
Datacenter Security *Asset Management*	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	
Datacenter Security *Controlled Access Points*	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Equipment Identification*	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security *Offsite Authorization*	DCS -04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	AWS Customers can designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Datacenter Security *Offsite equipment*	DCS -05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	In alignment with ISO 27001 standards, 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. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Policy*	DCS -06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS - 06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 and SOC 2 reports provides further information.
Datacenter Security *Secure Area Authorization*	DCS -07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	AWS Customers designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security *Unauthorized Persons Entry*	DCS -08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Datacenter Security *User Access*	DCS -09.1	Do you restrict physical access to information assets and functions by users and support personnel?	
Encryption & Key Management *Entitlement*	EKM -01.1	Do you have key management policies binding keys to identifiable owners?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key Management *Key Generation*	EKM -02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
	EKM - 02.2	Do you have a capability to manage encryption keys on behalf of tenants?	
	EKM - 02.3	Do you maintain key management procedures?	
	EKM - 02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	
	EKM - 02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	
Encryption & Key	EKM -03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key

Control Group	CID	Consensus Assessment Questions	AWS Response
Management *Encryption*	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	
Encryption & Key Management *Storage and Access*	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	
Governance and Risk Management *Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standards, Annex A, domain 14 and 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Governance and Risk Management *Risk Assessments*	GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS Customers. Continuous Monitoring of logical controls can be executed by customers on their own systems.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/.
Governance and Risk Management *Management Oversight*	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AWS provides our customers with our ISO 27001 certification. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how AWS internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the ISO 27001 certification standard. For additional information refer to the AWS Compliance ISO 27001 FAQ website: http://aws.amazon.com/compliance/iso-27001-faqs/.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	AWS has established information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external
Governance and Risk Management *Policy*	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance. Information about the AWS Compliance programs is published publicly on our website at http://aws.amazon.com/compliance/.
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management *Policy Enforcement*	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	AWS provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
Governance and Risk Management *Policy Reviews*	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Our AWS Cloud Security Whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security and http://aws.amazon.com/compliance, are updated on a regular basis to reflect updates to the AWS policies.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	The AWS SOC reports provide details related to privacy and security policy review.
Governance and Risk Management *Assessments*	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at aws.amazon.com/security) for additional details on AWS Risk Management Framework.

Control Group	CID	Consensus Assessment Questions	AWS Response
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	
Governance and Risk Management *Program*	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk. AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. AWS Risk Management program is reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	
Human Resources *Asset Returns*	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	AWS Customers retain the responsibility to monitor their own environment for privacy breaches. The AWS SOC reports provides an overview of the controls in place to monitor AWS managed environment.
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	
Human Resources *Background Screening*	HRS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. The AWS SOC reports provides additional details regarding the controls in place for background verification.
Human Resources *Employment Agreements*	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	In alignment with ISO 27001 standard, all AWS employees complete periodic role based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details. All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	
Human Resources *Employment Termination*	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. AWS SOC reports provide additional details.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Human Resources *Portable / Mobile Devices*	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Human Resources *Nondisclosure Agreements*	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.
Human Resources *Roles / Responsibilities*	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	The AWS Cloud Security Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security and http://aws.amazon.com/compliance.

Control Group	CID	Consensus Assessment Questions	AWS Response
Human Resources *Acceptable Use*	HRS -08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content. Refer to the ISO 27001 standard and 27018 code of practice for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 and ISO 27018.
	HRS - 08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	
	HRS - 08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	
Human Resources *Training / Awareness*	HRS -09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	HRS - 09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources *User Responsibility*	HRS -10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 7 and 8. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition the AWS Cloud Security Whitepaper provides further details - available at http://aws.amazon.com/security.
	HRS -10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS -10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources *Workspace*	HRS -11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8 and 9. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS -11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.
	HRS -11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	
Identity & Access Management *Audit Tools Access*	IAM -01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IAM -01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Identity & Access Management *User Access Policy*	IAM -02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM-02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored per the AWS access policy. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
Identity & Access Management *Policies and Procedures*	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	
Identity & Access Management *Segregation of Duties*	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Customers retain the ability to manage segregations of duties of their AWS resources. Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	
Identity & Access Management *Third Party Access*	IAM-07.1	Do you provide multi-failure disaster recovery capability?	AWS provides customers 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. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC reports provides further details. ISO 27001 standard Annex A, domain 15 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM-07.3	Do you have more than one provider for each service you depend on?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provided a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08.1	Do you document how you grant and approve access to tenant data?	AWS Customers retain control and ownership of their data. Controls in place limit access to systems and data and provide that 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 controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management *User Access Authorization*	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.
	IAM-09.2	Do you provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
Identity & Access Management *User Access Reviews*	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports. Refer to ISO 27001 standards, Annex A, domain 9 for additional details.

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM -10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM -10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	
Identity & Access Management *User Access Revocation*	IAM -11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM -11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	
Identity & Access Management *User ID Credentials*	IAM -12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa. AWS Identity and Access Management (IAM) supports identity federation for delegated access to the AWS Management Console or AWS APIs. With identity federation, external identities (federated users) are granted secure access to resources in your AWS account without having to create IAM users. These external identities can come from your corporate identity provider (such as Microsoft Active Directory or from the AWS Directory Service) or from a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google or any OpenID Connect (OIDC) compatible provider.
	IAM -12.2	Do you use open standards to delegate authentication capabilities to your tenants?	
	IAM -12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM -12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	
	IAM -12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM -12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	
	IAM -12.7	Do you allow tenants to use third-party identity assurance services?	
	IAM -12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/. AWS SOC reports provides details on the specific control activities executed by AWS.
	IAM -12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	
	IAM -12.10	Do you support the ability to force password changes upon first logon?	
	IAM -12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	
Identity & Access Management *Utility Programs Access*	IAM -13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides details on the specific control activities executed by AWS. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM -13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	
	IAM -13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	AWS Incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides additional details on controls in place to restrict system access. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	
	IVS-01.4	Are audit logs centrally stored and retained?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Details regarding AWS Service Limits and how to request an increase for specific services is available on the AWS website at http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html. AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
	IVS-04.3	Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website - http://aws.amazon.com/documentation/.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
	IVS-06.4	Are all firewall access control lists documented with business justification?	
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Interoperability & Portability *APIs*	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Details regarding AWS APIs can be found on the AWS website at https://aws.amazon.com/documentation/. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Interoperability & Portability *Data Request*	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	
Interoperability & Portability *Policy & Legal*	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.

Control Group	CID	Consensus Assessment Questions	AWS Response
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	AWS allows customers to move data as needed on and off AWS storage. Refer to http://aws.amazon.com/choosing-a-cloud-platform for more information on Storage options.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	
Interoperability & Portability *Virtualization*	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	
Mobile Security *Anti-Malware*	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional information.
Mobile Security *Application Stores*	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	AWS has established an information security framework and policies and has effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Mobile Security *Approved Applications*	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	
Mobile Security *Approved Software for BYOD*	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Mobile Security *Awareness and Training*	MOS -05	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	
Mobile Security *Cloud Based Services*	MOS -06	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	
Mobile Security *Compatibility*	MOS -07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security *Device Eligibility*	MOS -08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security *Device Inventory*	MOS -09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	
Mobile Security *Device Management*	MOS -10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security *Encryption*	MOS -11	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	
Mobile Security *Jailbreaking and Rooting*	MOS -12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Legal*	MOS -13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
	MOS -13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Lockout Screen*	MOS -14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security *Operating Systems*	MOS -15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	
Mobile Security *Passwords*	MOS -16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	
	MOS -16.2	Are your password policies enforced through technical controls (i.e. MDM)?	
	MOS -16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security *Policy*	MOS -17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	
	MOS -17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security *Remote Wipe*	MOS -18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	
	MOS -18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	
Mobile Security *Security Patches*	MOS -19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	
	MOS -19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	
Mobile Security *Users*	MOS -20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	
	MOS - 20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 and NIST 800-53 standards. Below is an outline of the three-phased approach AWS has implemented to manage incidents:
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including: - 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. - Trouble ticket entered by an AWS employee - 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 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. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow- up actions and end the call engagement. 3. Reconstitution Phase - Once 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 the internal communication mechanisms detailed above, 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" 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 our SOC, PCI DSS, ISO 27001 and FedRAMP compliance. **The AWS Cloud Security Whitepaper** available at http://aws.amazon.com/security provides additional details.
	SEF-02.4	Have you tested your security incident response plans in the last year?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of AWS services. Refer to AWS SOC report for specific details in relation to Data Integrity and Access Management (including least privilege access)
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC reports provides details on the specific control activities executed by AWS. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 15 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information. AWS does not generally outsource development of AWS services to subcontractors.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
	STA-05.3	Does legal counsel review all third-party agreements?	
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	STA-05.5	Do you provide the client with a list and copies of all sub processing agreements and keep this updated?	
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	AWS maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. AWS' third party management processes are reviewed by independent auditors as part of AWS ongoing compliance with SOC and ISO 27001.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	
Supply Chain Management, Transparency	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for

Control Group	CID	Consensus Assessment Questions	AWS Response
and Accountability *Third Party Audits*	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC reports provides additional details on the specific control activities executed by AWS.
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to AWS Cloud Security Whitepaper for further information - available at http://aws.amazon.com/security. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management *Mobile Code*	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	AWS allows customers to manage client and mobile applications to their own requirements.

Control Group	CID	Consensus Assessment Questions	AWS Response
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	

Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations

The Cloud Computing Security Considerations was created to assist agencies in performing a risk assessment of services offered by Cloud Service Providers. The following provides AWS alignment to the Security Considerations, published on September 2012. For additional details refer to: http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

Key Area	Questions	AWS RESPONSE
Maintaining Availability and Business Functionality	a. Business criticality of data or functionality. Am I moving business critical data or functionality to the cloud?	AWS customers retain control and ownership of their content. Customers are responsible for the classification and use of their content.
	b. Vendor's business continuity and disaster recovery plan. Can I thoroughly review a copy of the vendor's business continuity and disaster recovery plan that covers the availability and restoration of both my data and the vendor's services that I use? How much time does it take for my data and the services that I use to be recovered after a disaster, and do the vendor's other customers that are larger and pay more money than me get prioritization?	AWS customers retain control and ownership of their data. AWS provides customers 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. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. AWS provides customers 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. In case of failure, automated processes move customer data traffic away from the affected area. AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9 and the AWS SOC 1 Type II report for additional information.

Key Area	Questions	AWS RESPONSE
	c. My data backup plan. Will I spend additional money to maintain an up to date backup copy of my data located either at my agency's premises, or stored with a second vendor that has no common points of failure with the first vendor?	AWS customers retain control and ownership of their content and it is the customer's responsibility to manage their data backup plans. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website. AWS offers a range of cloud computing services to support Disaster Recovery. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/.
	d. My business continuity and disaster recovery plan. Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data center and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically "failover", so that if one vendor's services become unavailable, control is automatically and smoothly transitioned to the other vendor.	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. AWS 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 customers 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 that 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, they are each fed 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. Customers should architect their 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. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11 provides additional details. AWS has been validated

Key Area	Questions	AWS RESPONSE
		and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	e. My network connectivity to the cloud. Is the network connectivity between my agency's users and the vendor's network adequate in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss?	Customers can also choose their network path to AWS facilities, including multiple VPN endpoints in each AWS Region. In addition, AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	f. Vendor's guarantee of availability. Does the Service Level Agreement (SLA guarantee that the vendor will provide adequate system availability an quality of service, using their robust system architecture and business processes?	AWS does commit to high levels of availability in its service level agreements (SLAs). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.99% Service credits are provided in the case these availability metrics are not met. Customers should architect their 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. AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm].
	g. Impact of outages. Can I tolerate the maximum possible downtime of the SLA? Are the scheduled outage windows acceptable both in duration and time of day, or will scheduled outages interfere with my critical business processes?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
	h. SLA inclusion of scheduled outages. Does the SLA guaranteed availability percentage include scheduled outages?	AWS does not operate an environment with scheduled outage as AWS provides customers the ability to architect their environment to take advantage of multiple Availability Zones and regions.
	i. SLA compensation. Does the SLA adequately reflect the actual damage caused by a breach of the SLA such as unscheduled downtime or data loss?	AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS' Service Level Agreement.

Key Area	Questions	AWS RESPONSE
	j. Data integrity and availability. How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data?	AWS data integrity controls as described in AWS SOC 1 Type II report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 12 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. You choose where to store your data by specifying a region (for Amazon S3) or an availability zone within a region (for EBS). Data stored in Amazon Elastic Block Store (Amazon EBS) is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones. Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security
	k. Data restoration. If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA?	AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region.
	l. Scalability. How much available spare computing resources does the vendor provide to enable my usage of the vendor's services to scale at short notice?	The AWS cloud is distributed, highly secure and resilient, giving customers large scaling potential. Customers may scale up or down, paying for only what they use.

Key Area	Questions	AWS RESPONSE
	m. Changing vendor. If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business, how do I get access to my data in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? How do I ensure that my data is permanently deleted from the vendor's storage media? For Platform as a Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency?	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS.
Protecting Data from Unauthorized Access by a Third Party	a. Choice of cloud deployment model. Am I considering using a potentially less secure public cloud, a potentially more secure hybrid cloud or community cloud, or a potentially most secure private cloud?	AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet. Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center

Key Area	Questions	AWS RESPONSE
	b. Sensitivity of my data. Is my data to be stored or processed in the cloud classified, sensitive, private, or data that is publicly available such as information from my public web site? Does the aggregation of my data make it more sensitive than any individual piece of data? For example, the sensitivity may increase if storing a significant amount of data, or storing a variety of data that if compromised would facilitate identity theft. If there is a data compromise, could I demonstrate my due diligence to senior management, government officials and the public?	AWS customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements.
	c. Legislative obligations. What obligations do I have to protect and manage my data under various legislation, for example the Privacy Act, the Archives Act, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government?	AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers. AWS has published a whitepaper on using AWS in the context of Australian privacy considerations, available here.

Key Area	Questions	AWS RESPONSE
	d. Countries with access to my data. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centers? Will the vendor notify me if the answers to these questions change?	AWS customers choose the AWS Region or regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location of their choice. AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) region and store their content onshore in Australia. If the customer makes this choice, their content will be located in Australia unless the customer chooses to move the data. Customers can replicate and back up content in more than one region, but AWS does not move or replicate customer content outside of the customer's chosen region or regions. AWS is vigilant about customers' security and does not disclose or move data in response to a request from the Australian, U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-U.S. governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prevented from doing so.

Key Area	Questions	AWS RESPONSE
	e. Data encryption technologies. Are hash algorithms, encryption algorithms and key lengths deemed appropriate by the DSD ISM used to protect my data when it is in transit over a network, and stored on both the vendor's computers and on backup media? The ability to encrypt data while it is being processed by the vendor's computers is still an emerging technology and is an area of current research by industry and academia. Is the encryption deemed strong enough to protect my data for the duration of time that my data is sensitive?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance. The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSMs are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSMs near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive access to CloudHSMs, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your Amazon EC2 applications.
	f. Media sanitization. What processes are used to sanitize the storage media storing my data at its end of life, and are the processes deemed appropriate by the DSD ISM?	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. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	g. Vendor's remote monitoring and management. Does the vendor monitor, administer or manage the computers that store or process my data? If yes, is this performed remotely from foreign countries or from Australia? Can the vendor provide patch compliance reports and other details about the security of workstations used to perform this work, and what controls prevent the vendor's employees from using untrustworthy personally owned laptops?	Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.
	h. My monitoring and management. Can I use my existing tools for integrity checking, compliance checking, security monitoring and network management, to obtain visibility of all my systems regardless of whether these systems are located locally or in the cloud? Do I have to learn to use additional tools provided by the vendor? Does the vendor even provide such a mechanism for me to perform monitoring?	AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system performance and reliability, or help close security gap.
	i. Data ownership. Do I retain legal ownership of my data, or does it belong to the vendor and may be considered an asset for sale by liquidators if the vendor declares bankruptcy?	AWS customers retain ownership and control of their data. AWS only uses each customer's content to provide the AWS services selected by each customer to that customer and does not use customer content for any secondary purposes. AWS treats all customer content the same and has no insight as to what type of content the customer chooses to store in AWS. AWS simply makes available the compute, storage, database and networking services selected by customer – AWS does not require access to customer content to provide its services.

Key Area	Questions	AWS RESPONSE
	j. Gateway technologies. What technologies does the vendor use to create a secure gateway environment? Examples include firewalls, traffic flow filters, content filters, and antivirus software and data diodes where appropriate.	The AWS network provides significant protection against traditional network security issues and customers can implement further protection. Refer to the AWS Overview of Security whitepaper (available at http://aws.amazon.com/security) for additional details. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm].
	k. Gateway certification. Is the vendor's gateway environment certified against government security standards and regulations?	AWS obtains certain industry certifications and independent third-party attestations which include the AWS Gateway environment.
	l. Email content filtering. For email Software as a Service, does the vendor provide customizable email content filtering that can enforce my agency's email content policy?	A Customer can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available.

Key Area	Questions	AWS RESPONSE
	m. Policies and processes supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by policies and processes including threat and risk assessments, ongoing vulnerability management, a change management process that incorporates security, penetration testing, logging and regular log analysis, use of security products endorsed by the Australian Government, and compliance with Australian government security standards and regulations?	Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security. AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and formerly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment.
	n. Technologies supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by direct technical controls including timely application of security patches, regularly updated antivirus software, defense in depth mechanisms to protect against unknown vulnerabilities, hardened operating systems and software applications configured with the strongest possible security settings, intrusion detection and prevention systems,	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.

Key Area	Questions	AWS RESPONSE
	and data loss prevention mechanisms?	
	o. Auditing the vendor's IT security posture. Can I audit the vendor' implementation of security measures, including performing scans and other penetration testing of the environment provided to me? If there is justifiable reason why auditing is not possible, which reputable third party has performed audits and other vulnerability assessments? What sort of internal audits does the vendor perform, and which compliance standards and other recommended practices from organization's such as the Cloud Security Alliance are used for these assessments? Can I thoroughly review a copy of recent resulting reports?	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.

Key Area	Questions	AWS RESPONSE
	p. User authentication. What identity and access management systems does the vendor support for users to log in to use Software as a Service?	AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. AWS supports identity federation that makes it easier to manage users by maintaining their identities in a single place. AWS IAM includes support for the Security Assertion Markup Language (SAML) 2.0, an open standard used by many identity providers. This new feature enables federated single sign-on, or SSO, empowering users to log into the AWS Management Console or make programmatic calls to AWS APIs, by using assertions from a SAML-compliant identity provider, such as Shibboleth and Windows Active Directory Federation Services.
	q. Centralized control of data. What user training, policies and technical controls prevent my agency's users from using unapproved or insecure computing devices without a trusted operating environment to store or process sensitive data accessed using Software as a Service?	N/A

Key Area	Questions	AWS RESPONSE
	r. Vendor's physical security posture. Does the vendor use physical security products and devices that are endorsed by the Australian Government? How is the vendor's physical data center designed to prevent the tampering or theft of servers, infrastructure and the data stored thereon? Is the vendor's physical data center accredited by an authoritative third party?	The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations AWS provides data center physical access and information to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls. Refer to ISO 27001 standard, Annex A, domain 9 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	s. Software and hardware procurement. What procurement process is used to ensure that cloud infrastructure software and hardware has been supplied by a legitimate source and has not been maliciously modified in transit?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standard, Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by the Vendor's Customers	a. Customer segregation. What assurance do I have that the virtualization and "multi-tenancy" mechanisms guarantee adequate logical and network segregation between multiple tenants, so that a malicious customer using the same physical computer as me cannot access my data?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
	b. Weakening my security posture. How would using the vendor's cloud infrastructure weaken my agency's existing network security posture? Would the vendor advertise me as one of their customers without my explicit consent, thereby assisting an adversary that is specifically targeting me?	AWS customers are considered confidential and would not advertise customer details without explicit consent. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
	c. Dedicated servers. Do I have some control over which physical computer runs my virtual machines? Can I pay extra to ensure that no other customer can use the same physical computer as me e.g. dedicated servers or virtual private cloud?	VPC allows customers to launch Amazon EC2 instances that are physically isolated at the host hardware level; they will run on single tenant hardware. A VPC can be created with 'dedicated' tenancy, in which case all instances launched into the VPC will utilize this feature. Alternatively, a VPC may be created with 'default' tenancy, but customers may specify 'dedicated' tenancy for particular instances launched into the VPC.
	d. Media sanitization. When I delete portions of my data, what processes are used to sanitize the storage media before it is made available to another customer, and are the processes deemed appropriate by the DSD ISM?	Customers retain ownership and control of their content and provide customers with the ability to delete their data. 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. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by Rogue Vendor Employees	a. Data encryption key management. Does the vendor know the password or key used to decrypt my data, or do I encrypt and decrypt the data on my computer so the vendor only ever has encrypted data?	AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
	b. Vetting of vendor's employees. What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities.
	c. Auditing vendor's employees. What robust identity and access management system do the vendor's employees use? What auditing process is used to log and review the actions performed by the vendor's employees?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
	d. Visitors to data center. Are visitors to data centers escorted at all times, and is the name and other personal details of every visitor verified and recorded?	All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is routinely logged and audited.
	e. Physical tampering by vendor's employees. Is network cabling professionally installed to Australian standards or internationally acceptable standards, to help avoid the vendor's employees from accidentally connecting cables to the wrong computers, and to help readily highlight any deliberate attempts by the vendor's employees to tamper with the cabling?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. This includes appropriate protection for network cables. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
	f. Vendor's subcontractors. Do the answers to these questions apply equally to all of the vendor's subcontractors?	Provisioning contractor / vendor access is managed the same for both employees and contractors, with responsibility shared across Human Resources (HR), Corporate Operations and Service Owners. Vendors are subject to the same access requirements as employees.
Handling Security Incidents	a. Timely vendor support. Is the vendor readily contactable and responsive to requests for support, and is the maximum acceptable response time captured in the SLA or simply a marketing claim that the vendor will try their best? Is the support provided locally, or from a foreign country, or from several foreign countries using an approach that follows the sun? What mechanism does the vendor use to obtain a real-time understanding of the security posture of my use of the vendor's services so that the vendor can provide support?	AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers. The service helps customers of all sizes and technical abilities to successfully utilize the products and features provided by Amazon Web Services. All AWS Support tiers offer customers of AWS Infrastructure Services an unlimited number of support cases with pay-by-the-month pricing and no long-term contracts. The four tiers provide developers and businesses the flexibility to choose the support tiers that meet their specific needs.
	b. Vendor's incident response plan. Does the vendor have a security incident response plan that specifies how to detect and respond to security incidents, in a way that is similar to incident handling procedures detailed in the DSD ISM? Can I thoroughly review a copy?	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 and NIST 800-53 standards. Below is an outline of the three-phased approach AWS has implemented to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including: - 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. - Trouble ticket entered by an AWS employee - 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 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. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow- up actions and end the call engagement.

		3. Reconstitution Phase - Once 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 the internal communication mechanisms detailed above, 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" 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 our SOC, PCI DSS, ISO 27001 and FedRAMP compliance. **The AWS Cloud Security Whitepaper** available at http://aws.amazon.com/security provides additional details.
	c. Training of vendor's employees. What qualifications, certifications and regular information security awareness training do the vendor's employees require, to know how to use the vendor's systems in a secure manner and to identify potential security incidents?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	d. Notification of security incidents. Will the vendor notify me via secure communications of security incidents that are more serious than an agreed threshold, especially in cases where the vendor might be liable? Will the vendor automatically notify law enforcement or other authorities, who may confiscate computing equipment used to store or process my data?	Notification of security incidents are handled on a case-by-case basis and as required by applicable law. Any notification is performed via secure communications.
	e. Extent of vendor support. How much assistance will the vendor provide me with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	AWS provides infrastructure and customers manage everything else, including the operating system, the network configuration and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
	f. My access to logs. How do I obtain access to time synchronized audit logs and other logs to perform a forensic investigation, and how are the logs created and stored to be suitable evidence for a court of law?	Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. Refer to aws.amazon.com/cloudtrail for additional details. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	g. Security incident compensation. How will the vendor adequately compensate me if the vendor's actions, faulty software or hardware contributed to a security breach?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.

Key Area	Questions	AWS RESPONSE
	h. Data spills. If data that I consider is too sensitive to be stored in the cloud is accidentally placed into the cloud, referred to as a data spill, how can the spilled data be deleted using forensic sanitization techniques? Is the relevant portion of physical storage media zeroed whenever data is deleted? If not, how long does it take for deleted data to be overwritten by customers as part of normal operation, noting that clouds typically have significant spare unused storage capacity? Can the spilled data be forensically deleted from the vendor's backup media? Where else is the spilled data stored, and can it be forensically deleted?	Customers retain ownership and control of their content. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.

Appendix C: Glossary of Terms

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

DSS: The Payment Card Industry Data Security Standard (DSS) is a worldwide information security standard assembled and managed by the Payment Card Industry Security Standards Council.

EBS: Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

FedRAMP[sm]: The Federal Risk and Authorization Management Program (FedRAMP[sm]) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP[sm] is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels.

FISMA: The Federal Information Security Management Act of 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FIPS 140-2: The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information.

GLBA: The Gramm–Leach–Bliley Act (GLB or GLBA), also known as the Financial Services Modernization Act of 1999, sets forth requirements for financial institutions with regard to, among other things, the disclosure of nonpublic customer information and the protection of threats in security and data integrity.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

IAM: AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

ITAR: International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Government agencies and contractors must comply with ITAR and restrict access to protected data.

ISAE 3402: The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

ISO 9001: AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

ISO 27001: ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

NIST: National Institute of Standards and Technology. This agency sets detailed security standards as needed by industry or government programs. Compliance with FISMA requires agencies to adhere to NIST standards.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

PCI: Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

QSA: The Payment Card Industry (PCI) Qualified Security Assessor (QSA) designation is conferred by the PCI Security Standards Council to those individuals that meet specific qualification requirements and are authorized to perform PCI compliance assessments.

SAS 70: Statement on Auditing Standards No. 70: Service Organizations is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization (such as AWS) and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. The SAS 70 report has been replaced by the Service Organization Controls 1 report.

Service: Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

Service Level Agreement (SLA): A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

SOC 1: Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (formerly referred to as the SSAE 16 report), is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The

international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16 [deprecated]: The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

SOC 2: Service Organization Controls 2 (SOC 2) reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.

SOC 3: Service Organization Controls 3 (SOC 3) reports are designed to meet the needs of uses who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 Reports can be freely distributed or posted on a website as a seal.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

Version History

January 2016
- Added GxP Compliance Program
- Twelfth region added (Asia Pacific - Seoul)

December 2015
- Updates to certifications and third-party attestations summaries
- Added ISO 27017 certification
- Added ISO 27018 certification
- Eleventh region added (China - Beijing)

November 2015
- Update to CSA v3.0.1

August 2015
- Updates to in-scope services for PCI 3.1
- Updates to regions in-scope for PCI 3.1

May 2015
- Tenth region added (EU - Frankfurt)
- Updates to in-scope services for SOC 3
- SSAE 16 language deprecated

Apr 2015
- Updates to in-scope services for: FedRAMP[sm], HIPAA, SOC 1, ISO 27001, ISO 9001

Feb 2015
- Updates to FIPS 140-2 VPN endpoints and SSL-terminating load balancers
- Updates to PCI DSS verbiage

Dec 2014
- Updates to certifications and third-party attestations summaries

Nov 2013 version
- Edits to IPsec tunnel encryption verbiage

Jun 2013 version
- Updates to certifications and third-party attestations summaries
- Updates to Appendix C: Glossary of Terms
- Minor changes to formatting

Jan 2013 version
- Edits to certifications and third-party attestations summaries

Nov 2012 version
- Edits to content and updated certification scope
- Added reference to the SOC 2 and MPAA

Jul 2012 version
- Edits to content and updated certification scope
- Addition of the CSA Consensus Assessments Initiative Questionnaire (Appendix A)

Jan 2012 version
- Minor edits to content based on updated certification scope

- Minor grammatical edits

Dec 2011 version

- Change to Certifications and Third-party Attestation section to reflect SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, and FIPS 140-2
- Addition of S3 Server Side Encryption
- Added additional cloud computing issue topics

May 2011 version

- Initial release

Notices

ATTACHMENT E

AWS Access Policy – State
(v.1-4-2013)

This AWS Access Policy ("**Access Policy**") governs your access to and use of the Services (as defined below) of Amazon Web Services, Inc. ("**AWS**") provided to you by your systems integrator, reseller, or services provider ("**Provider**"). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent ("**you**") for use of the Services. In this Access Policy, "**we**", "**us**", or "**our**" means AWS and any of its affiliates. Please see Section 10 for definitions of capitalized terms.

1. Use of the Services.

1.1 Generally. You are provided access to the Services by your Provider. Your use of and access to the Services are governed by the agreement between you and Provider. This Access Policy supplements the terms of such agreement and may updated by us from time to time. AWS Service Level Agreements do not apply to your use of the Services. Your continued access to and use of the Services is conditioned on your compliance with all laws, rules, regulations, policies and instructions applicable to your use of the Services, including the Policies.

1.2 Account Keys. Provider may provide you with AWS account keys which will allow you to directly access the Services via Provider's account(s). We are not responsible for any activities that occur under these account keys, regardless of whether the activities are undertaken by you, Provider or a third party (including your employees, contractors or agents) and we are also not responsible for unauthorized access to the account.

1.3 Third Party Materials. Through the use of Provider's AWS account(s), you may have access to Third Party Materials, such as software applications provided by third parties, which are made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Your use of any Third Party Materials is at your sole risk.

2. Your Responsibilities

2.1 Your Materials. You are solely responsible for the development, content, operation, maintenance, and use of Your Materials with the Services. For example, you are solely responsible for:

(a) the technical operation of Your Materials, including ensuring that calls you make to any Service are compatible with then-current application program interfaces for that Service;

(b) compliance of Your Materials with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Materials;

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act;

(e) any action that you permit, assist or facilitate any person or entity to take related to this Access Policy, Your Materials or use of the Services; and

(f) End Users' use of Your Materials and the Services and ensuring that End Users comply with your obligations under this Access Policy and that the terms of your agreement with each End User are consistent with this Access Policy.

2.2 Other Security and Backup. You or Provider are solely responsible for properly configuring and using the Services and taking steps to maintain appropriate security, protection and backup of Your Materials, including using encryption technology to protect Your Materials from unauthorized access

and routinely archiving Your Materials.

2.3 End User Violations. If you become aware of any violation of your obligations under this Access Policy by an End User, you will immediately terminate such End User's access to Your Materials and the Services.

3. Service Interruption.

3.1 General. We may suspend the AWS account(s) through which you access the Services immediately if we determine your or an End User's use of the Services (i) violates the terms of this Access Policy (including the Acceptable Use Policy or Service Terms); (ii) poses a security risk to the Services or any other AWS customer, (iii) may harm our systems or the systems or Materials of any other AWS customer; or (iv) may subject us to liability as a result of any of the foregoing. We will provide notice of any suspension as soon as practicable to Provider, who is solely responsible for providing any notices to you under your agreement with them.

3.2 Scope of Interruption. To the extent practicable, we will (i) suspend your right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected. Nothing in this Section 3 will operate to limit your rights or remedies otherwise available to you against Provider under your agreement with them or applicable law.

4. Proprietary Rights

4.1 Services. As between you and us, we or our licensors own and reserve all right, title, and interest in and to the Services. You have the right to use the Services solely as a licensee of Provider in accordance with this Access Policy and the agreement between you and Provider. We have no obligation to provide the Service to you under this Access Policy, so you must look exclusively to Provider and your agreement with Provider regarding such obligation. Except as expressly provided in this Section 4, you obtain no rights to the Services, the AWS Materials or any Third Party Materials.

4.2 Materials. As a part of the Services, you may have access to AWS Materials and Third Party Materials, which may be subject to additional terms and conditions (including the Terms of Use and Apache Software License). By using those materials, you are subject to such additional terms. You are solely responsible for securing any necessary approvals for the download and use of such materials.

4.3 Restrictions. Neither you nor any End User may use the Services in any manner or for any purpose other than as expressly permitted by this Access Policy and the agreement between you and Provider. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas. All rights and access granted to you with respect to the Services are conditioned on your continued compliance with this Access Policy, and you will immediately discontinue your use of the Services if you cannot comply with this Access Policy. You will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Services or AWS Materials that you have used.

4.4 Suggestions. If you provide any Suggestions to us when using the Services, you hereby grant to AWS and its affiliates a perpetual, irrevocable, non-exclusive, worldwide, royalty-free right and license to reproduce, distribute, make derivative works based upon, publicly display, publicly perform, make, have made, use, sell, offer for sale, and import the Suggestions, including the right to sublicense such rights through multiple tiers, alone or in combination.

4.5 Government Rights. If you are using the Services on behalf of the government and these terms fail to meet the government's needs or are inconsistent in any respect with federal or state law, you will immediately discontinue your use of the Services (including any AWS Materials).

5. Representations and Warranties. You represent and warrant that (a) you and your End Users' use of the Services (including any use by your employees and personnel) will not violate this Access Policy; (b) you or your licensors own all right, title, and interest in and to Your Materials; (c) Your Materials (including the use, development, design, production, advertising, or marketing of your Materials) or the combination of your Materials 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) your use of the Services will not cause harm to any End User.

6. Indemnification. Except to the extent prohibited by applicable state law, you will defend, indemnify, and hold harmless us, our licensors and each of our respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to any third party claim concerning: (a) your or any End Users' use of the Services (including use by your employees and personnel); (b) Your Materials or the combination of Your Materials with other applications, content or processes, including any claim involving alleged infringement or misappropriation of third-party rights or the use, development, design, production, advertising or marketing of Your Materials; or (c) a dispute between you and any End User. If your ability to comply with the foregoing provision is limited to any extent by the absence of appropriations or government authorization, you will make good faith efforts to obtain sufficient appropriations or authorization for any liabilities arising under this Section 5.

7. Disclaimers. WE PROVIDE THE SERVICES ON AN "AS IS" BASIS TO PROVIDER. WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO YOU, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING YOUR MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

8. Limitations of Liability. YOU MUST LOOK SOLELY TO PROVIDER AND YOUR AGREEMENT WITH THEM REGARDING ANY CLAIMS OR DAMAGES RELATED TO THE SERVICES. WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) SUSPENSION OF YOUR USE OF OR ACCESS TO THE SERVICES, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICES, OR, (III) ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; OR (B) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR MATERIALS OR OTHER DATA THAT YOU OR ANY END USER SUBMITS OR USES IN CONNECTION WITH THE SERVICES (INCLUDING AS A RESULT OF YOUR OR ANY END USERS' ERRORS, ACTS OR OMISSIONS).

9. Miscellaneous.

9.1 Governing Law; Venue. Except to the extent prohibited by applicable state law, the laws of the State of Washington, without reference to conflict of law rules, govern this Access Policy and any dispute of any sort that might arise between you and us. You irrevocably consent to exclusive jurisdiction and venue of the federal courts located in King County, Washington with respect to any

dispute arising in connection with the Services or this Access Policy. We may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply.

9.2 Entire Agreement. This Access Policy is the entire agreement between you and us regarding the Services, including any materials. It supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us, whether written or verbal, regarding the subject matter of this Access Policy. If the terms of this document are inconsistent with the terms contained in your agreement with Provider, the terms contained in this document will control. We will not be bound by, and specifically object to, any term, condition or other provision which is different from or in addition to the provisions of this Access Policy (whether or not it would materially alter it) and which is submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document.

9.3 Survival. The following provisions will survive any termination of your use of the Services: Sections 2.1, 4, 5, 6, 7, 8, 9 and 10.

10. Definitions.

"Acceptable Use Policy" means the policy currently available at http://aws.amazon.com/aup, as it may updated by us from time to time.

"AWS Materials" means Materials we make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Materials does not include the Services.

"AWS Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time.

"AWS Site" means http://aws.amazon.com and any successor or related site designated by us.

"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 User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Materials; or (b) otherwise accesses or uses the Services through you.

"Materials" means software (including machine images), data, text, audio, video, images or other content.

"Policies" means the Acceptable Use Policy, the Terms of Use, the Service Terms, all restrictions described in the AWS Materials and on the AWS Site, and any other policy or terms referenced in or incorporated into this Access Policy.

"Services" means, collectively or individually (as applicable), the web services made commercially available by us to Provider for use under this Access Policy, including (as applicable) those web services described in the Service Terms.

"Service Terms" means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms, as they may be updated by us from time to time.

"Suggestions" means all suggested improvements to the Services or AWS Materials that you provide to us.

"Terms of Use" means the terms of use located at http://aws.amazon.com/terms/, as they may be updated by us from time to time.

"Third Party Materials" means Materials made available to you by any third party on the AWS Site or in conjunction with the Services.

"Your Materials" means Materials you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services or otherwise transfer, process, use or store in connection with the Services.

Microsoft Cloud Agreement

This Microsoft Cloud Agreement is between the entity you represent, or, if you do not designate an entity in connection with a Subscription purchase or renewal, you individually ("you" or "your"), and Microsoft Corporation ("Microsoft", "we", "us", or "our"). It consists of the terms and conditions below, as well as the Online Services Terms, and the SLA (together, the "agreement"). It is effective on the date that your Reseller provisions your Subscription. Key terms are defined in Section 11.

1. Use of Online Services.

a. Right to use. We grant you the right to access and use the Online Services and to install and use the Software included with your Subscription, as further described in this agreement. We reserve all other rights.

b. Choosing a Reseller. You must choose and maintain a Reseller authorized within your region. If Microsoft or Reseller chooses to discontinue doing business with each other, you must choose a replacement Reseller or purchase a Subscription directly from Microsoft, which may require you to accept different terms.

c. Reseller Administrator Access and Customer Data. You acknowledge and agree that (i) once you have 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, you may request additional administrator privileges from your Reseller; (ii) Reseller's privacy practices with respect to Customer Data or any services provided by Reseller may differ from Microsoft's privacy practices; and (iii) Reseller may collect, use, transfer, disclose, and otherwise process Customer Data, including personal data. You consent to Microsoft providing Reseller with Customer Data and information that you provide to Microsoft for purposes of ordering, provisioning and administering the Online Services.

d. Acceptable use. You may use the Product only in accordance with this agreement. You may not reverse engineer, decompile, disassemble, or work around technical limitations in the Product, except to the extent applicable law permits it despite these limitations. You may not disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters your use of the Online Services. You may not rent, lease, lend, resell, transfer, or host the Product, or any portion thereof, to or for third parties except as expressly permitted in the Online Services Terms.

e. End Users. You control access by End Users, and you are responsible for their use of the Product in accordance with this agreement. For example, you will ensure End Users comply with the Acceptable Use Policy.

f. Customer Data. You are solely responsible for the content of all Customer Data. You will secure and maintain all rights in Customer Data necessary for us to provide the Online Services to you without violating the rights of any third party or otherwise obligating Microsoft to you or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to your use of the Product other than as expressly set forth in this agreement or as required by applicable law.

g. Responsibility for your accounts. You are responsible for maintaining the confidentiality of any non-public authentication credentials associated with your use of the Online Services. You must promptly notify customer support about any possible misuse of your accounts or authentication credentials or any security incident related to the Online Services.

h. Eligibility for Academic, Government and Nonprofit versions. You agree that if you are purchasing an academic, government or nonprofit offer, you meet 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.

i. Preview releases. We 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. We may change or discontinue Previews at any time without notice. We also may choose not to release a Preview into "General Availability."

2. Subscriptions, ordering.

a. Available Subscription offers. The Subscription offers available to you will be established by your Reseller and generally can be categorized as one or a combination of the following:

(i) Commitment Offering. You commit in advance to purchase a specific quantity of Online Services for use during a Term and to pay upfront or on a periodic basis in advance of use.

(ii) Consumption Offering (also called Pay-As-You-Go). You pay based on actual usage with no upfront commitment.

(iii) Limited Offering. You receive 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.

b. Ordering.

(i) Orders must be placed through your designated Reseller. You may place orders for your Affiliates under this agreement and grant your Affiliates administrative rights to manage the Subscription, but, Affiliates may not place orders under this agreement. You also may assign the rights granted under Section 1.a to a third party for use by that third party in your internal business. If you grant any rights to Affiliates or third parties with respect to Software or your Subscription, such Affiliates or third parties will be bound by this agreement and you agree to be jointly and severally liable for any actions of such Affiliates or third parties related to their use of the Products.

(ii) Your Reseller may permit you 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.

c. Pricing and payment. Prices for each Product and any terms and conditions for invoicing and payment will be established by your Reseller.

d. Renewal.

(i) Upon renewal of your Subscription, you may be required to sign a new agreement, a supplemental agreement or an amendment to this agreement.

(ii) Your Subscription will automatically renew unless you provide your Reseller with notice of your intent not to renew prior to the expiration of the Term.

e. 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, and suspension.

a. Agreement term and termination. This agreement will remain in effect until the expiration or termination of your Subscription, whichever is earliest. You may terminate this agreement at any time by contacting your Reseller. The expiration or termination of this agreement will only terminate your right to place new orders for additional Products under this agreement.

b. Cancellation or transfer of Subscription. Your Reseller will establish the terms and conditions, if any, upon which you may cancel or transfer a Subscription.

c. Suspension. We may suspend your use of the Online Services if: (1) it is reasonably needed to prevent unauthorized access to Customer Data; (2) you fail to respond to a claim of alleged infringement under Section 6 within a reasonable time; or (3) you do not abide by the Acceptable Use Policy or you violate other terms of this agreement. If one or more of these conditions occurs, then:

(i) For Limited Offerings, we may suspend your use of the Online Services or terminate your Subscription and your account immediately without notice.

(ii) For all other Subscriptions, a suspension will apply to the minimum necessary part of the Online Services and will be in effect only while the condition or need exists. We will give notice to the named administrators for your Subscription, which may be you and/or your Reseller, before we suspend, except where we reasonably believe we need to suspend immediately. If you do not fully address the reasons for the suspension within 60 days after we suspend, we may terminate your Subscription and delete your Customer Data without any retention period. We may also terminate your Subscription if your use of the Online Services is suspended more than twice in any 12-month period.

4. Security, privacy, and data protection.

a. You consent to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. You 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. You will obtain all required consents from third parties under applicable privacy and data protection laws before providing personal information to Microsoft.

b. 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 your Reseller.

c. You consent and authorize Microsoft (and its service providers and subcontractors), at Reseller's direction or as required by law, to access and disclose to law enforcement or other government authorities data from, about or related to you, including the content of communications (or to provide law enforcement or other government entities access to such data).

d. As and to the extent required by law, you 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 you shall obtain the users' consent to the same.

e. You appoint Reseller as your agent for purposes of interfacing with and providing instructions to Microsoft for purposes of this Section 4.

5. Warranties.

a. Limited warranty.

(i) Online Services. We warrant that the Online Services will meet the terms of the SLA during the Term. Your only remedies for breach of this warranty are those in the SLA.

(ii) Software. We warrant for one year from the date you first use the Software that it will perform substantially as described in the applicable user documentation. If Software fails to meet this warranty we will, at our option and as your exclusive remedy, either (1) return the price paid for the Software or (2) repair or replace the Software.

b. Limited warranty exclusions. This limited warranty is subject to the following limitations:

(i) any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law will last one year from the start of the limited warranty;

(ii) this limited warranty does not cover problems caused by accident, abuse or use of the Products in a manner inconsistent with this agreement or our published documentation or guidance, or resulting from events beyond our reasonable control;

(iii) this limited warranty does not apply to problems caused by a failure to meet minimum system requirements; and

(iv) this limited warranty does not apply to Previews or Limited Offerings.

c. DISCLAIMER. Other than this warranty, we provide no warranties, whether express, implied, statutory, or otherwise, including warranties of merchantability or fitness for a particular purpose. These disclaimers will apply except to the extent applicable law does not permit them.

6. Defense of claims.

a. Defense.

(i) We will defend you against any claims made by an unaffiliated third party that a Product infringes that third party's patent, copyright or trademark or makes unlawful use of its trade secret.

(ii) You will defend us against any claims made by an unaffiliated third party that (1) any Customer Data, Customer Solution, or Non-Microsoft Products, or services you provide, directly or indirectly, in using a Product infringes the third party's patent, copyright, or trademark or makes unlawful use of its trade secret; or (2) arises from violation of the Acceptable Use Policy.

b. Limitations. Our obligations in Section 6.a won't apply to a claim or award based on: (i) any Customer Solution, Customer Data, Non-Microsoft Products, modifications you make to the Product, or services or materials you provide or make available as part of using the Product; (ii) your combination of the Product with, or damages based upon the value of, Customer Data, or a Non-Microsoft Product, data, or business process; (iii) your use of a Microsoft trademark without our express written consent, or your use of the Product after we notify you to stop due to a third-party claim; (iv) your redistribution of the Product to, or use for the benefit of, any unaffiliated third party; or (v) Products provided free of charge.

c. Remedies. If we reasonably believe that a claim under Section 6.a.(i) may bar your use of the Product, we will seek to: (i) obtain the right for you to keep using it; or (ii) modify or replace it with a functional equivalent and notify you to stop use of the prior version of the Product. If these options are not commercially reasonable, we may terminate your rights to use the Product and then refund any advance payments for unused Subscription rights.

d. Obligations. Each party must notify the other promptly of a claim under this Section 6. The party seeking protection must (i) give the other sole control over the defense and settlement of

the claim; and (ii) give reasonable help in defending the claim. The party providing the protection will (1) reimburse the other for reasonable out-of-pocket expenses that it incurs in giving that help and (2) pay the amount of any resulting adverse final judgment or settlement. The parties' respective rights to defense and payment of judgments (or settlement the other consents to) under this Section 6 are in lieu of any common law or statutory indemnification rights or analogous rights, and each party waives such common law or statutory rights.

7. Limitation of liability.

a. Limitation. The aggregate liability of each party for all claims under this agreement is limited to direct damages up to the amount paid under this agreement for the Online Service during the 12 months before the cause of action arose; provided, that in no event will a party's aggregate liability for any Online Service exceed the amount paid for that Online Service during the Subscription. For Products provided free of charge, Microsoft's liability is limited to direct damages up to $5,000.00 USD.

b. EXCLUSION. Neither party will be liable for loss of revenue or indirect, special, incidental, consequential, punitive, or exemplary damages, or damages for lost profits, revenues, business interruption, or loss of business information, even if the party knew they were possible or reasonably foreseeable.

c. Exceptions to limitations. 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. Software.

a. Additional Software for use with the Online Services. To enable optimal access and use of certain Online Services, you may install and use certain Software in connection with your use of the Online Service. The number of copies of the Software you will be permitted to use or the number of devices on which you will be permitted to use the Software will be as described in the Online Services Terms in the product specific license terms for the Online Service. We may check the version of the Software you are using and recommend or download updates, with or without notice, to your devices. Failure to install updates may affect your ability to use certain functions of the Online Service. You must uninstall the Software when your right to use it ends. We may also disable it at that time. Your rights to access Software on any device do not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that access that device.

b. License confirmation. Proof of your Software license is (1) this agreement, (2) any order confirmation, and (3) proof of payment.

c. License rights are not related to fulfillment of Software media. Your acquisition of Software media or access to a network source does not affect your license to Software obtained under this agreement. We license Software to you, we do not sell it.

d. Transferring and assigning licenses. License transfers are not permitted.

9. Support.

Support services for Products purchased under this agreement will be provided by your Reseller.

10. Miscellaneous.

a. Notices. You must send notices by mail, return receipt requested, to the address below.

Notices should be sent to:	Copies should be sent to:
Microsoft Corporation Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329	Microsoft Corporation Legal and Corporate Affairs 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. 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.

h. 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 Microsoft Online Subscription Agreement, (2) the Online Services Terms, and (3) any other documents in this agreement.

i. Survival. The terms in Sections 1, 2.e, 5, 6, 7, 10 and 11 will survive termination or expiration of this agreement.

j. U.S. export jurisdiction. The Products are subject to U.S. export jurisdiction. You must comply with all applicable 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. For additional information, see http://www.microsoft.com/exporting/.

k. 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.

l. 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.

11. 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.

"Customer Solution" 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, or any user of a Customer Solution.

"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 terms that apply to your use of the Products available at http://www.microsoft.com/licensing/onlineuserights. The Online Services Terms include terms governing your use of Products that are in addition to the terms in this agreement.

"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 any Online Service (including any Software).

"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 the commitments we make regarding delivery and/or performance of an Online Service, as published at http://www.microsoftvolumelicensing.com/csla, or at an alternate site that we identify.

"Software" means software we provide for installation on your device as part of your Subscription or to use with the Online Service to enable certain functionality.

"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).