



Contract # AR2484

STATE OF UTAH COOPERATIVE CONTRACT

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

InfoReliance Corporation
Name
4050 Legato Road, Suite 700
Address
Fairfax VA 22033
City State Zip

LEGAL STATUS OF CONTRACTOR

- ☐ Sole Proprietor
☐ Non-Profit Corporation
☒ For-Profit Corporation
☐ Partnership
☐ Government Agency

Contact Person Theresa Grouge Phone #703-246-9360, ext 1162 Email Theresa.grouge@inforeliance.com
Vendor #VC205715 Commodity Code #920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed
3. PROCUREMENT PROCESS: This contract is entered into as a result of the procurement process on Bid#CH16012.
4. CONTRACT PERIOD: Effective Date: 10/14/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.
6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
ATTACHMENT E: AWS Public Sector Access Policy, AWS Service Terms, and Drafting Ordering Instructions and Template
- Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.**
8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
b. Utah State Procurement Code and the Procurement Rules.
9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

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

CONTRACTOR

STATE

[Signature]
Contractor's signature Date 10/7/2016

[Signature]
Director, Division of Purchasing Date 10.31.16

Theresa Grouge, Director of Contracts
Type or Print Name and Title

<u>Christopher Hughes</u> Division of Purchasing Contact Person	<u>801-538-3254</u> Telephone Number	<u></u> Fax Number	<u>christopherhughes@utah.gov</u> 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 Addendum¹ ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits² 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 SaaS.

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 Office³.

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 shown in Attachment F.

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

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

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

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

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

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

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 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.

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.

Attachment H – 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	Not Offered	Not Offered	Not Offered	None
IaaS	Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon EC2 Container Service	Amazon EC2 Container Service	Amazon EC2 Container Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Lambda	AWS Lambda	AWS Lambda	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Auto Scaling	AWS Auto Scaling	AWS Auto Scaling	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Elastic Load Balancing	Elastic Load Balancing	Elastic Load Balancing	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Virtual Private Cloud (Amazon VPC)	Amazon Virtual Private Cloud (Amazon VPC)	Amazon Virtual Private Cloud (Amazon VPC)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Route 53	Amazon Route 53	Amazon Route 53	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Direct Connect	AWS Direct Connect	AWS Direct Connect	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Glacier	Amazon Glacier	Amazon Glacier	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Elastic Block Store (Amazon EBS)	Amazon Elastic Block Store (Amazon EBS)	Amazon Elastic Block Store (Amazon EBS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudFront	Amazon CloudFront	Amazon CloudFront	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

IaaS	AWS Import/Export	AWS Import/Export	AWS Import/Export	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Storage Gateway	AWS Storage Gateway	AWS Storage Gateway	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon DynamoDB	Amazon DynamoDB	Amazon DynamoDB	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Redshift	Amazon Redshift	Amazon Redshift	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon ElastiCache	Amazon ElastiCache	Amazon ElastiCache	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Elastic MapReduce (Amazon EMR)	Amazon Elastic MapReduce (Amazon EMR)	Amazon Elastic MapReduce (Amazon EMR)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Kinesis	Amazon Kinesis	Amazon Kinesis	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Data Pipeline	AWS Data Pipeline	AWS Data Pipeline	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Mobile Analytics	Amazon Mobile Analytics	Amazon Mobile Analytics	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Identity and Access Management (IAM)	AWS Identity and Access Management (IAM)	AWS Identity and Access Management (IAM)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Directory Service	AWS Directory Service	AWS Directory Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Service Catalog	AWS Service Catalog	AWS Service Catalog	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Config	AWS Config	AWS Config	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudHSM	AWS CloudHSM	AWS CloudHSM	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

IaaS	AWS Key Management Service (KMS)	AWS Key Management Service (KMS)	AWS Key Management Service (KMS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudTrail	AWS CloudTrail	AWS CloudTrail	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudWatch	Amazon CloudWatch	Amazon CloudWatch	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Management Console	AWS Management Console	AWS Management Console	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Command Line Interface (CLI)	AWS Command Line Interface (CLI)	AWS Command Line Interface (CLI)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	APIs	APIs	APIs	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Elastic Beanstalk	AWS Elastic Beanstalk	AWS Elastic Beanstalk	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudFormation	AWS CloudFormation	AWS CloudFormation	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodeDeploy	AWS CodeDeploy	AWS CodeDeploy	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodeCommit	AWS CodeCommit	AWS CodeCommit	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodePipeline	AWS CodePipeline	AWS CodePipeline	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS OpsWorks	AWS OpsWorks	AWS OpsWorks	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon WorkDocs	Amazon WorkDocs	Amazon WorkDocs	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon WorkSpaces	Amazon WorkSpaces	Amazon WorkSpaces	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon AppStream	Amazon AppStream	Amazon AppStream	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudSearch	Amazon CloudSearch	Amazon CloudSearch	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

IaaS	Amazon Simple Workflow Service (Amazon SWF)	Amazon Simple Workflow Service (Amazon SWF)	Amazon Simple Workflow Service (Amazon SWF)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Queue Service (Amazon SQS)	Amazon Simple Queue Service (Amazon SQS)	Amazon Simple Queue Service (Amazon SQS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Email Service (Amazon SES)	Amazon Simple Email Service (Amazon SES)	Amazon Simple Email Service (Amazon SES)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Notification Service (Amazon SNS)	Amazon Simple Notification Service (Amazon SNS)	Amazon Simple Notification Service (Amazon SNS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Elastic Transcoder	Amazon Elastic Transcoder	Amazon Elastic Transcoder	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Cognito	Amazon Cognito	Amazon Cognito	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Flexible Payments Service (Amazon FPS)	Amazon Flexible Payments Service (Amazon FPS)	Amazon Flexible Payments Service (Amazon FPS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Support	AWS Support	AWS Support	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Trusted Advisor	AWS Trusted Advisor	AWS Trusted Advisor	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
PaaS	Not Offered	Not Offered	Not Offered	None

info|RELIANCE

STATE OF UTAH DIVISION OF PURCHASING NASPO VALUEPOINT CLOUD SOLUTIONS

SUBMITTED TO:

State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Mr. Christopher Hughes
Assistant Director
christopherhughes@utah.gov
(801) 538-3254

SUBMITTED BY:

InfoReliance Corporation
4050 Legato Road, Suite 700
Fairfax, VA 22033

Ms. Theresa Grouge
Director of Contracts
Theresa.grouge@infoeliance.com
(703) 246-9360, x1162 (phone)
(703) 246-9331 (fax)

Table of Contents

Section 9: Cost Proposal Introduction	1
9.1 Cloud Solution	1
9.2 Catalog Pricing	2
9.3 Catalog Discounts.....	2
9.4 Support Services Pricing.....	2
9.5 Services Discounts	3
9.6 Escalation	3
9.7 Travel and Other Direct Costs	3
9.8 Validity Period	3
9.9 Period of Performance.....	3

Section 9: Cost Proposal Introduction

InfoReliance is pleased to submit this cost proposal in response to Solicitation CH16012 to provide cloud solutions to the State of Utah / National Association of State Procurement Officials (NASPO) ValuePoint. The following sections detail our price narrative and incorporate information requested in **RFP Attachment G**, specifically in **Section 9.3** and **Section 9.4**. We also provide a minimum discount to satisfy the pass/fail scoring requirement from RFP 4.3.3. Our prices are inclusive of the 0.25% NASPO ValuePoint Administration Fee.

9.1 Cloud Solution

InfoReliance offers a premier solutions-focused partnership with significant experience in cloud computing. We also leverage our reputation and experience in providing the most efficient, cost effective, innovative, and compliant solutions delivered in a timely manner to our public sector, healthcare, and commercial customers. InfoReliance helps make the transition to Cloud computing **easy, effortless, and smooth**.

InfoReliance is focused on innovation and deliberate engineering transformation. We effectively balance innovation and discipline. Our background as a premier SharePoint solutions and software development partner enables us to lead the way for our customers in moving their mission critical applications and workloads to the cloud. Our knowledge of cloud computing and engineering models, strong partnership with Amazon Web Services (AWS), and our proven pre- and post-deployment support infrastructure allows us to successfully deliver cloud solutions to our customers.

InfoReliance is an Amazon Advanced Consulting Partner and Lead Partner for Amazon in building the AWS SharePoint QuickStart and Rapid Deployment methodology. Our AWS practice is comprised of more than 10 AWS Certified Solution Architects, 50 AWS trained and accredited technical staff and more than 60 AWS trained and accredited business staff.



To ensure a structured and controlled migration to AWS cloud, InfoReliance has developed an Cloud framework. Our cloud consulting services and solutions follow this repeatable framework that includes comprehensive lifecycle activities related to Vision, Requirements, Design, Provision, Migration, Testing, Change Management, and Support.

InfoReliance offers innovative AWS cloud solutions to the federal government based on the following core competencies:

- ▶ **Cloud Service Solutions:** InfoReliance offers a full lifecycle of cloud solutions based on a proven framework and methodology to include:
 - Design, optimization, and configuration
 - Architecture solutioning
 - Cloud road-mapping
 - Return on investment (ROI) and business case analysis
 - Enterprise application development and data migration to the cloud
 - Knowledge transfer and training
 - 24x7x365 cloud support service center

InfoReliance is a lead global AWS partner in their test drive and quick start platforms.

- ▶ **Expert Solutions Architects:** InfoReliance currently has 13+ AWS Certified Solutions Architects, 39+ AWS certified technical professionals, and 60+ AWS certified business professionals. Our team has extensive experience in designing and implementing complex configuration and architectures through hands on expertise and cost effective solutioning.

- **AWS Innovation Lab:** InfoReliance offers a fully functional AWS Innovation Lab for testing, developing, and deploying environments. Key activities include:
- Evaluation of emerging & beta AWS technology releases
 - Proofs of concept and demo environments
 - Development of AMLs and deployment templates to expedite solutions
 - Test drive environments for customer evaluations

InfoReliance provides and manages a number of AWS proofs of concept for Federal customers to help them evaluate cloud offerings in the context of their business.

- **Information Assurance (IA) Expertise:** InfoReliance maintains a team of highly skilled and trained IA staff with industry certifications and Authority to Operate (ATO) practical hands on experience supporting Federal customers. Our knowledge library contains ATO templates and best practice case studies.

9.2 Catalog Pricing

InfoReliance is offering NASPO a minimum **2% discount off of the AWS list price**. This matches our GSA Contract pricing. By providing a discount off of list price, we are always able to pass along any price reductions immediately as they occur. The current list prices are published on the following URL: <http://aws.amazon.com/pricing/> or located in the AWS calculator at: <http://calculator.s3.amazonaws.com/index.html>.

9.3 Catalog Discounts

AWS is consistently publishing price reductions on a monthly basis to their product offerings. On Jan 13th, 2016, AWS had its 52nd price reduction since its inception. InfoReliance will capture these reductions at the time of offer and will adjust any additional reductions as they occur through the billing phase of the contract. The minimum discount for our offerings are listed in the table below.

Cloud Solution by Category	Minimum Discount
Software as a Service	2.00%
Infrastructure as Service	2.00%
Platform as a Service	2.00%

9.4 Support Services Pricing

InfoReliance reviewed the requirements for the service areas required. We then took the requirements and mapped them against our commercial price list to the most appropriate labor category. Based on this analysis, we determined applicable discounts and applied a 2.00% discount to our Remote site rate and 7.00% to our Onsite rate (rates listed in the table below). While the table below reflects our ceiling rates in accordance with the proposal instructions, InfoReliance will reflect the highest discount possible on all orders through the life of the 10 year contract.

Functional Area	Labor Category	Onsite	Remote
Maintenance Services	Information Technology Specialist 3	\$73.47	\$77.42
Deployment Services	Application Support 3	\$155.31	\$163.66
Consulting Services	Senior Consultant 1	\$202.74	\$213.64
Architectural Design Services	Senior Consultant 1	\$202.74	\$213.64
Statement of Work Services	Consultant 1	\$159.03	\$167.58
Partner Services	Technical Expert 1	\$247.38	\$260.68
Training Deployment Services	Training Specialist 3	\$139.50	\$147.00

9.5 Services Discounts

We anticipate offering additional discounts at the individual order level based on the labor dollar value, duration, contract type, and requirements of the individual task orders issued against this contract.

Our prices are inclusive of the 0.25% NASPO ValuePoint Administration Fee.

9.6 Escalation

InfoReliance used a 2% salary escalation effective the beginning of each option period.

We are proposing a 2% escalation as this is the percentage change for the 12-months that ended December 2015 for all private industry workers excluding incentive paid occupations. This information can be found in the December 2015 BLS Employment Cost Index; specifically, Table 5. Employment Cost Index for total compensation, for private industry workers, by occupational group and industry (Not seasonally adjusted).

9.7 Travel and Other Direct Costs

InfoReliance will identify and propose any travel as required to perform on any resulting task orders under this ID/IQ.

InfoReliance will identify and propose any Other Direct Costs (ODCs) as required to perform on any resulting task orders under this ID/IQ. General and Administrative rates are applied to ODCs in accordance with our standard accounting practices. We will not charge a fee on ODCs.

9.8 Validity Period

InfoReliance's proposal is valid for one hundred and twenty (120) days to the Government from the proposal date.

9.9 Period of Performance

The Master agreement will be for ten (10) years with no renewal periods.

info|RELIANCE

STATE OF UTAH DIVISION OF PURCHASING NASPO VALUEPOINT CLOUD SOLUTIONS

SUBMITTED TO:

State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Mr. Christopher Hughes
Assistant Director
christopherhughes@utah.gov
(801) 538-3254

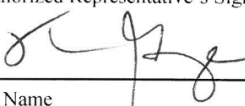
SUBMITTED BY:

InfoReliance Corporation
4050 Legato Road, Suite 700
Fairfax, VA 22033

Ms. Theresa Grouge
Director of Contracts
Theresa.grouge@infoeliance.com
(703) 246-9360, x1162 (phone)
(703) 246-9331 (fax)



State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable) InfoReliance Corporation		Federal Tax Identification Number 54-1979520		State of Utah Sales Tax ID Number	
Ordering Address 4050 Legato Road, Suite 700		City Fairfax	State VA	Zip Code 22033	
Remittance Address (if different from ordering address)		City	State	Zip Code	
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation		Company Contact Person Ms. Theresa Grouge			
Telephone Number (include area code) (703) 246.9360 x1162		Fax Number (include area code) (703) 246.9331			
Company's Internet Web Address www.inforeliance.com		Email Address theresa.grouge@inforeliance.com			
Offeror's Authorized Representative's Signature 					
Type or Print Name Theresa Grouge					
Position or Title of Authorized Representative Director of Contracts					
Date: 3/10/2016					

12/15/2014

Table of Contents

1. RFP Signature Page.....	i
2. Executive Summary.....	1
3. Mandatory Minimums	4
3.1. (M) Signature Page (RFP 5.1)	4
3.2. (M) Cover Letter (RFP 5.2)	4
3.3. (M) Acknowledgment of Amendments (RFP 5.3)	6
3.4. (M) Executive Summary (RFP 5.4).....	7
3.5. (M) General Requirements for the Service Offerings (RFP 5.5)	7
3.5.1. Provide a Usage Report Administrator (RFP 5.5.1).....	7
3.5.2. Cooperate with NASPO and SciQuest (RFP 5.5.2).....	7
3.5.3. Maintain Completed CSA STAR Registry Self-Assessment (RFP 5.5.3)	7
3.5.4. Sample of Service Level Agreement (RFP 5.5.4).....	8
3.6. Recertification of Mandatory Minimums (RFP 5.7)	8
4. Business Profile	9
4.1. (M)(E) Business Profile (RFP 6.1)	9
4.2. (M)(E) Scope of Experience (RFP 6.2).....	10
4.3. (M) Financials (6.3).....	12
4.4. (E) General Information (RFP 6.4).....	12
4.4.1. Depth and Breadth of Solutions in Cloud Marketplace (RFP 6.4.1).....	12
4.4.2. Auditing Capabilities and Reports Consistent with SAS 70 (RFP 6.4.2).....	16
4.5. (E) Billing and Pricing Practices (RFP 6.5)	17
4.5.1. Billing and Pricing Practices, Including Transparency (6.5.1).....	17
4.5.2. Typical Cost Impacts (RFP 6.5.2).....	20
4.5.3. NIST Compliant (RFP 6.5.3).....	21
4.6. (E) Scope and Variety of Cloud Solutions (RFP 6.6)	23
4.7. (E) Best Practices (RFP 6.7)	24
5. Organization Profile	28
5.1. (M)(E) Contract Manager (RFP 7.1)	28
5.1.1. Contract Manager Point of Contact and Work Hours (RFP 7.1.1)	28
5.1.2. Contract Manager Detailed Experience and Resume (RFP 7.1.2)	28
5.1.3. Contract Manager Roles and Responsibilities (RFP 7.1.3)	30
6. Technical Response	32
6.1. (M)(E) Technical Requirements (RFP 8.1)	33
6.1.1. Cloud Service Models and Deployment Models (RFP 8.1.1).....	33
6.1.2. How Solutions Meet NIST Essential Characteristics (RFP 8.1.2).....	97
6.1.3. Solution Subcategories (RFP 8.1.3).....	100
6.1.4. Willingness to Comply With Attachments C & D (RFP 8.1.4)	101
6.1.5. Adherence to Attachment D, Scope of Services (RFP 8.1.5)	101
6.2. (E) Subcontractors (RFP 8.2)	101

6.2.1. Detailed Plans for Providing Services (RFP 8.2.1)	101
6.2.2. Subcontractors to Perform Contract Requirements (RFP 8.2.2)	102
6.2.3. Subcontractor Qualifications (RFP 8.2.3)	102
6.3. (E) Working with Purchasing Entities (RFP 8.3)	102
6.3.1. Working with Purchasing Entities (RFP 8.3.1)	102
6.3.2. Adware, Unauthorized Software, and Unauthorized Marketing (RFP 8.3.2)	104
6.3.3. Application Hosting Environments (RFP 8.3.3)	104
6.3.4. Accessibility Policies (RFP 8.3.4)	104
6.3.5. Applications Accessible Using Multiple Browser Platforms (RFP 8.3.5)	105
6.3.6. Meeting with the Purchasing Entity (RFP 8.3.6)	105
6.3.7. Project Schedule and Work Plans (RFP 8.3.7)	105
6.4. (E) Customer Service (RFP 8.4)	105
6.4.1. Ensuring Excellent Customer Service	105
6.4.2. Ability to Comply with Customer Service Requirements (RFP 8.4.2)	107
6.5. (E) Security of Information (RFP 8.5)	107
6.5.1. Agreements to Protect Data (RFP 8.5.1)	107
6.5.2. Data Privacy and Security (RFP 8.5.2)	108
6.5.3. Conditions to Access User Accounts or Data (RFP 8.5.3)	108
6.6. (E) Privacy and Security (RFP 8.6)	109
6.6.1. NIST Compliance (RFP 8.6.1)	109
6.6.2. Security Certifications (RFP 8.6.2)	109
6.6.3. Security Practices (RFP 8.6.3)	110
6.6.4. Data Confidentiality Standards and Practices (RFP 8.6.4)	111
6.6.5. List of Third-party Attestations, Reports, Security Credentials and Certifications (RFP 8.6.5)	112
6.6.6. Logging Process (RFP 8.6.6)	113
6.6.7. Visibility of Cloud Hosted Data and Documents and Restriction to Specific Users or Groups (RFP 8.6.7)	115
6.6.8. Incident Response Notification Process (RFP 8.6.8)	116
6.6.9. Security Controls Used to Isolate Hosted Servers (RFP 8.6.9)	116
6.6.10. Security Technical Reference Architectures (RFP 8.6.10)	116
6.6.11. Security Procedures (RFP 8.6.11)	118
6.6.12. Security Measures and Standards for Confidentiality of Data (RFP 8.6.12)	118
6.6.13. Policies and Procedures for Data Breach Notifications (RFP 8.6.13)	118
6.7. Migration and Redeployment Plan (RFP 8.7)	118
6.7.1. End of Life Activities (RFP 8.7.1)	118
6.7.2. Return of Data (RFP 8.7.2)	118
6.8. (E) Service or Data Recovery (RFP 8.8)	118
6.8.1. Response to Situations (RFP 8.8.1)	119
6.8.2. Methodologies for Backup and Restore Services (RFP 8.8.2)	121
6.9. (E) Data Protection (RFP 8.9)	124

6.9.1. Standard Encryption Technologies / Protecting Sensitive Data (RFP 8.9.1)	124
6.9.2. Business Associate Agreements (RFP 8.9.2)	125
6.9.3. How InfoReliance Will Use Data (RFP 8.9.3)	125
6.10.(E) Service Level Agreements (RFP 8.10)	126
6.10.1. Negotiable Service Level Agreement (RFP 8.10.1)	126
6.10.2. Sample of Service Level Agreement (RFP 8.10.2)	126
6.11.(E) Data Disposal (RFP 8.11)	126
6.12.(E) Performance Measures and Reporting (RFP 8.12)	127
6.12.1. Guaranteed Reliability and Uptime (RFP 8.12.1)	127
6.12.2. Standard Uptime and SLA Criteria (RFP 8.12.2)	127
6.12.3. Support Contact (RFP 8.12.3)	127
6.12.4. Consequences/SLA Remedies for Incidents (RFP 8.12.4)	127
6.12.5. Downtime Procedures and Schedules (RFP 8.12.5)	129
6.12.6. Consequences/SLA Remedies for Disaster Recovery (RFP 8.12.6)	129
6.12.7. Sample of Performance Reports (RFP 8.12.7)	129
6.12.8. Ability to Print Reports Locally (8.12.8)	130
6.12.9. On-demand Deployment Support (RFP 8.12.9)	130
6.12.10. Scale-up and Scale-down Availability (RFP 8.12.10)	131
6.13.(E) Cloud Security Alliance (RFP 8.13)	132
6.14.(E) Service Provisioning (8.14)	132
6.14.1. Emergency or Rush Services Implementation Requests (RFP 8.14. 1)	133
6.14.2. Standard Lead-time for Provisioning Solutions (RFP 8.14.2)	133
6.15.(E) Backup and Disaster Plan (RFP 8.15)	133
6.15.1. Apply Retention Periods and Disposition (RFP 8.15.1)	133
6.15.2. Disaster Recovery Risks and Mitigation (RFP 8.15.2)	133
6.15.3. Infrastructure that Supports Multiple Data Centers (RFP 8.15.3)	133
6.16.(E) Solution Administration (8.16)	134
6.16.1. Management of Identity and User Accounts (RFP 8.16.1)	134
6.16.2. Anti-Virus Protection (RFP 8.16.2)	134
6.16.3. Migrating Data (RFP 8.16.3)	134
6.16.4. Ability to Administer Solution (RFP 8.16.4)	135
6.16.5. Ability to Apply Defined Administration Policies (RFP 8.16.5)	135
6.17.(E) Hosting and Provisioning (RFP 8.17)	135
6.17.1. Cloud Hosting and Provisioning Process (RFP 8.17.1)	135
6.17.2. Minimum Toolsets (RFP 8.17.2)	136
6.18.(E) Trial and Testing Periods (Pre-And Post-Purchase) (RFP 8.18)	137
6.18.1. Testing and Training Periods (RFP 8.18.1)	137
6.18.2. Test and/or Proof of Concept Environment for Evaluation (RFP 8.18.2)	137
6.18.3. Training and Support at No Additional Cost (RFP 8.18.3)	137
6.19.(E) Integration and Customization (RFP 8.19)	138

6.19.1. Solutions Integrated to Complementary Applications (RFP 8.19.1).....	138
6.19.2. Customize and Personalize the Solutions (RFP 8.19.2).....	138
6.20.(E) Marketing Plan (RFP 8.20)	138
6.21.(E) Related Value-Added Services to Cloud Solutions (RFP 8.21).....	139
6.21.1. Professional Services for Initial Setup, Training, and Access to Services	139
6.21.2. Related Services for Optional Use by Participating Entities	140
6.22.(E) Supporting Infrastructure (RFP 8.22).....	144
6.22.1. Infrastructure Required by Purchasing Entity (RFP 8.22.1).....	144
6.22.2. Responsibility for Installation of New Infrastructure (RFP 8.22.2).....	144
6.23.(E) Alignment of Cloud Computing Reference Architecture (RFP 8.23)	144

Table of Figures

Figure 1: 2015 Gartner Magic Quadrant for Cloud IaaS.....	15
Figure 2: Forrester Wave™ Public Cloud Service Providers' Security, Q4 '14.....	16
Figure 3: Billing Dashboard.....	19
Figure 4: Scope and Variety of AWS Cloud Solutions by Subcategory.....	24
Figure 5: AWS Marketplace.....	27
Figure 6: Contracts Organization with Interfaces.....	31
Figure 7: NIST Cloud Essential Characteristics:	97
Figure 8: AWS Management Console.....	98
Figure 9: AWS Management Console.....	98
Figure 10: AWS Services and Solution Subcategories.....	100
Figure 11: Representative Project Plan.....	105
Figure 12: Solution Delivery Framework	106
Figure 13: AWS Security Reference Architecture.....	117
Figure 14: Spectrum of Disaster Recovery Options.....	120
Figure 15: Traditional Backup Approach.....	122
Figure 16: Amazon EC2 Backup Approach.....	123
Figure 17: Sample Performance Report (Real Time).....	129
Figure 18: Sample Performance Report (Historical).....	130
Figure 19: Accessing the Full List of Services.....	131
Figure 20: How to Access a List of Available Services in a Category.....	131
Figure 21: InfoReliance Cloud Migration Framework.....	142
Figure 22: The AWS Migration Continuum.....	143

2. Executive Summary

Offeror must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

InfoReliance is a leading national provider of cloud solutions to the public sector based on the Amazon Web Services (AWS) Infrastructure as a Service (IaaS). We are pleased to offer NASPO ValuePoint and the Participating Entities from 32 States a complete catalog of AWS IaaS offerings and value added services that **meet or exceed all of NASPO's minimum mandatory requirements as well as the evaluated technical qualifications**. InfoReliance is offering a minimum discount from list price on all IaaS offerings with the added benefit that **all AWS cost reductions will be passed on to the customer in real time without delay**. This is significant because AWS continues to drive cloud costs downward. In 2014, AWS reduced the cost of compute by an average of 30%, storage by an average of 51%, and relational databases by an average of 28%. **InfoReliance will pass AWS price reductions on to NASPO immediately** by applying the discount structure to real time AWS pricing. For ease of evaluation, InfoReliance is also taking **no exceptions to the terms and conditions of the NASPO Master Agreement**.

InfoReliance Quick Facts

- ▶ 300+ Employees / \$100M+ 2015 Revenue
- ▶ 30+ contracts deploying cloud and Amazon Web Services (AWS) and Microsoft cloud solutions
- ▶ \$1B+ in services delivered to 60+ Government Agencies
- ▶ AWS Channel Reseller
- ▶ AWS GSA Schedule 70 Reseller
- ▶ AWS NASA SEWP and NITAAC CIO-CS GWAC Reseller
- ▶ AWS Advanced Consulting Partner with Microsoft Competency
- ▶ AWS Managed Service Provider (MSP) Audited June 2015
- ▶ 2014 AWS Simplify and Invent Partner of the Year
- ▶ AWS Government and Test Drive Partner
- ▶ AWS Customer Advisory Board Member
- ▶ CMMI Level 3, ISO 20000:270001 certified
- ▶ 2014 Microsoft Solutions Provider of the Year and six time Partner of the Year
- ▶ Microsoft SharePoint Partner of the Year
- ▶ Microsoft Office 365 Design and Deployment Partner
- ▶ Microsoft Azure Circle and Cloud Deployment Partner
- ▶ Azure CSP Tier 1 Reseller
- ▶ Azure Managed Service Provider (MSP)
- ▶ Azure Customer Advisory Board Member

NASPO Scope of Services: InfoReliance is not proposing any Platform as a Service (PaaS) or Software as a Service (SaaS) offerings at this time. All 53 AWS IaaS offerings can be deployed in each these National Institute of Standards and Technology (NIST) deployment models: Private, Public, or Hybrid. Most of the offerings can also be deployed in the fourth NIST deployment model (Community). InfoReliance and AWS are fully capable of storing and securing data at all three risk levels as defined by Federal Information Processing Standards (FIPS) PUB 199 (Low Risk Data, Moderate Risk Data, High Risk Data).

AWS IaaS Platform Expertise: Leading analysts like Gartner have consistently recognized AWS as the world's leading IaaS platform offering fully on-demand, any time access to true cloud utility services from a web browser. Every technology service provided in a data center is now available from AWS in a true on-demand, pay as you go, fully scalable model with far superior security controls. InfoReliance has delivered and deployed AWS solutions since 2011 and is a leading provider of cloud solutions to Government entities. InfoReliance is an **AWS Authorized Government Reseller, Advanced Consulting Partner, and fully audited Managed Service Partner (MSP)**. We are excited to make our years of investment and expertise available to NASPO so it can be leveraged across mission critical workloads and objectives.



AWS Innovation Expertise: InfoReliance has demonstrated a relentless obsession for cloud innovation and excellence. Examples include hosting individual initiatives on AWS for early adopters of the cloud, establishing a cloud sandbox for the Health and Human Services (HHS) Office of the Chief Information Officer (OCIO), and a recent \$45M contract with the National Archives and Records Administration (NARA) for AWS IaaS and PaaS on a managed services model. ***This proven success will directly benefit the Participating Entities*** under the NASPO Cloud Solutions Master Agreement. As we market our offerings, we will share use cases and lessons learned to help inform their buying decisions.

Public Sector Expertise: InfoReliance has implemented cloud-based solutions for 30+ public sector customers. Our extensive knowledge of delivering cloud solutions to the US public sector will allow NASPO Participating Entities to leverage our experience with cloud security compliance, cyber security, data classification and protection, continuous monitoring, risk management frameworks, and certifications such as FedRAMP, FISMA, HIPAA, CJIS, and ITAR. Our current AWS customers include the Department of Defense (Army, Air Force, and Marine Corps), cabinet level agencies (Health and Human Services, Department of Labor, Department of Interior, and Department of Justice) as well as individual agencies (Tennessee Valley Authority, Federal Bureau of Investigations, Bureau of Prisons, and Federal Communications Commission). We understand public sector requirements for high availability, secure, on-demand cloud services and are a nationally recognized leader in deploying value added AWS IaaS cloud solutions.

Cloud Value Added Services Expertise: InfoReliance can also go beyond the value-added services in the Master Agreement for interested Participating Entities. Examples include developing a cloud roadmap, refactoring applications, application and data migration with a proven cloud migration framework, or implementing a managed services model. These additional services are described in detail in **Section 6.21.2**.

Large Business Expertise with small business focus: InfoReliance is a ***financially stable, fiscally responsible large business*** with \$100M+ annual revenue in each of the last five years and more than \$1B since 2000. We have the equivalent of a Duns and Bradstreet 3A2 rating and an impeccable financial history. As the prime contract holder, ***we will provide IaaS offerings at the highest service levels, greatest security, maximum flexibility, and lowest possible risk*** to the Participating entities. Our size also enables us to intimately understand and focus on our customer's core missions and invest the time and resources to become a true partner to achieve these objectives.

Multiple Award Cloud Expertise: As a large business, InfoReliance has the existing infrastructure to manage a multiple-award contract for a consortium as large as NASPO. This includes a dedicated Program Management Office (PMO) for the two largest Government Wide Acquisition Contracts (GWACS) as well as GSA IT Schedule 70 task orders for AWS and commercial sales. Currently InfoReliance is providing cloud solutions to customers through over \$250M in multi year flexible ordering agreement awards and we have dedicated resources to process orders, provision AWS instances, and provide customer service up to 24/7/365. We recently completed an ISO 9001 audit that includes our billing and purchasing practices. We have extensive experience negotiating AWS terms and conditions for different contract structures. All of this means ***the Participating Entities can complete orders quickly and efficiently*** in accordance with the best interest of the Government. InfoReliance already sells each of the proposed AWS IaaS offerings on NASA SEWP V (\$20B ceiling), NITAAC CIO-CS (\$20B ceiling), GSA IT Schedule 70, NETCENTS 2 Application Services (F/O), and several agency-wide BPAs and IDIQs. ***Our NASPO Contract Manager has more than five years experience managing some of the largest cloud services contracts ever awarded by the Federal Government*** and 23 years contracts management experience overall.

Cloud Cost Savings Expertise: Through our optimized procurement and innovative cloud platforms, InfoReliance has assisted customers in recognizing cost savings through a reduction in compute and storage hardware, software licensing, and streamlined resource provisioning and management of IT resources. These savings have been reallocated by our customers into mission critical support areas such as software application modernization at the FBI and increased health and wellness grants at HHS. In 2015, the International Data Corporation (IDC) published a whitepaper discussing how 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. As a leading public sector AWS strategic partner, InfoReliance has the necessary experience and expertise to work with customers to recognize these same scale of savings and realize the value benefit of cloud computing. As described in detail in **Section 4.5.1** and in our cost proposal, we can apply our minimum discount structure to real time AWS pricing so that NASPO Purchasing Entities can immediately take advantage of AWS price reductions. This is a significant advantage over standard Government cloud contracts like GSA IT Schedule 70.

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

Cloud Invoice Expertise: AWS billing and attributable cost accounting for Government customers is a unique function that requires years of expertise. InfoReliance manages statutory and regulatory concerns, fee-for-service arrangements, security policies, contract administration, and allocated and aggregated reporting across projects and organizations. InfoReliance has developed ISO frameworks to ensure customers receive timely and accurate invoices.

24x7 Technical Incident Support Expertise: NASPO requires expert incident resolution 24x7x365 and AWS offers the most comprehensive SLA backed support. This includes flexible packages based on the needs of the customer and dedicated Technical Account Managers if required to ensure the highest levels of technical

Cloud Customer Service Expertise: To complement AWS Technical support, InfoReliance offers customers a world class, dedicated, and fully accredited AWS cloud customer service support to ensure the highest levels of overall customer satisfaction every day. Our staff just does cloud—and that enables InfoReliance to offer services such as AWS configuration and optimization to customers in addition to standard administrative support.

Cloud Adoption Life Cycle Expertise: Many of our customers initially require just AWS resale. As they increase their consumption, customers often request cloud consulting services support to develop optimized architectures or for specialized cloud services like Big Data. In addition, many customer then opt for a fully managed services MSP model in which InfoReliance provides the resale, consulting, software licenses, application development all within a recurring monthly fee and backed by guaranteed service level agreements. Whatever path a customer selects, InfoReliance is there to offer convenient and flexible services and support throughout the cloud adoption lifecycle to meet any needs.

InfoReliance is fully committed to meeting all of NASPO Participating Entities needs for Cloud Solutions from Day One and leveraging our extensive cloud expertise serving the public sector with world class AWS IaaS solutions.

3. Mandatory Minimums

In accordance with the instructions in **RFP Section 3.12 (para. 3)**, this section includes point by point responses to each item described in **RFP Section 5**. For convenience, we have also included a compliance table for all minimum mandatory requirements:

#	Minimum Mandatory Requirements	RFP Section	Evaluation	Proposal Section(s)
1	Signature Page	5.1	PASS	Pg. i, Section 3.1
2	Cover Letter	5.2	PASS	Section 3.2
3	Acknowledgement of Amendments	5.3	PASS	Section 3.3
4	Executive Summary	5.4	PASS	Sections 2 and 3.4
5	General Requirements	5.5	PASS	Section 3.5
6	Recertification	5.8	PASS	Section 3.6
7	Business Profile	6.1	PASS	Section 4.1
8	Scope of Experience	6.2	PASS	Section 4.2
9	Financials	6.3	PASS	Section 4.3, 7.0
10	Contract Manager	7.1	PASS	Section 5.1
11	Cost Proposal Submitted	9.1	PASS	Cost Proposal (Section 9)

In addition to submitting a Cost Proposal, we also comply with the pass/fail requirement in **RFP Section 4.3.3** by providing a minimum discount for our Cloud Solutions.

3.1.(M) Signature Page (RFP 5.1)

Excluded from this section per RFP Section 3.12 (para. 3).

We have included the signed Vendor Information Page at the front of our proposal and we will also complete the electronic version as part of the BidSync submission process.

3.2.(M) Cover Letter (RFP 5.2)

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 [statements 5.2.1 through 5.2.6].*

10 March 2016

Mr. Christopher Hughes, Assistant Director
State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Re: CH16012 – Cloud Solutions

Mr. Hughes:

InfoReliance is pleased to submit our proposal for Cloud Solutions in response to the NASPO ValuePoint RFP CH16012 dated 21 Dec 2015, with proposal submissions due 10 March 2016 by 3:00 PM EST. InfoReliance has an unparalleled track record for technical excellence and exceptional customer service in providing a full range of Cloud Solutions and services.

Our full proposal includes the following files. Major proposal documents (except the redacted version of Section 7) have the solicitation number and title, our company name, and the submission date appended to the file name.

1. Technical Proposal (**Sections 1-6**)
 - a. **Attachment A** – AWS Risk and Compliance Whitepaper

- b. **Attachment B** – AWS Sample SLAs
 - c. **Attachment C** – AWS Letter of Support
 - d. **Attachment D** – AWS ISO 27001 Certification
 - e. **Attachment H** – InfoReliance Identification of Service Models
2. Protected Information (**Section 7**) – Protected Business Confidential
3. Protected Information (**Section 7**) – Redacted Version
4. **Attachment E** – InfoReliance Claim of Business Confidentiality
5. Exceptions or Additions (**Section 8**)
 - a. **Attachment F** – AWS Service Terms 22 Feb 2016
 - b. **Attachment G** – AWS Public Sector Access Policy
 - c. **Attachment I** – Draft Ordering Instructions and Template
6. Cost Proposal (**Section 9 + RFP Attachment G**) – this document includes a narrative response to RFP Section 9.1 and incorporates Attachment G – Cost Schedule)

The primary Point of Contact for this proposal is our Director of Contracts, Ms. Theresa Grouge:

InfoReliance Corporation
4050 Legato Road Suite 700
Fairfax, VA 22033

Ms. Theresa Grouge
Director of Contracts
theresa.grouge@infoeliance.com
(703) 246.9360 ext. 1162 (tel)
(703)246.9331 (fax)

The following statements are in response to **RFP Subsections 5.2.1** through **5.2.6**.

(RFP 5.2.1) InfoReliance confirms our understanding that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

(RFP 5.2.2) The primary authors for this proposal are InfoReliance employees. Our Fulfillment Partner, Amazon Web Services (AWS), also provided a partner package describing their cloud services. InfoReliance incorporated these service descriptions into the proposal response.

(RFP 5.2.3) InfoReliance confirms it is not currently suspended, debarred, or otherwise excluded from Federal or State procurement and non-procurement programs.

(RFP 5.2.4) InfoReliance acknowledges that a 0.25% NASPO ValuePoint Administrative Fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

(RFP 5.2.5) InfoReliance is categorizing all cloud-based services under the terms of this RFP as Infrastructure as a Service (IaaS). All of the IaaS offerings support the NIST Private, Public, and Hybrid deployment models. Most offerings also support Community cloud. These offerings are defined in detail, including available deployment models and service model subcategories, in **Section 6.1.1** and **Attachment H – InfoReliance Identification of Service Models**.

(RFP 5.2.6) InfoReliance and AWS are capable of storing and securing data at all three risk levels as defined by FIPS PUB 199 (Low Risk Data, Moderate Risk Data, High Risk Data). The US East and US West regions hold a Provisional Authorization for level 2 which permits mission owners to deploy public, unclassified information in these regions with both the AWS Authorization and the mission application's ATO. The AWS GovCloud (US) region now holds a Provisional

Authorization for levels 2 and 4 and permits mission owners to deploy the full range of controlled, unclassified information categories covered by these levels. This is demonstrated in **Section 4.4.1** and specified for each service offering in **Attachment H – InfoReliance Identification of Service Models**.

E-Rate (RFP 3.15) USAC recently changed the Service Provider Identification Number (SPIN) to 498 ID. InfoReliance is an active participant in the program and **our 498 ID is 143048656**.

InfoReliance thanks the State of Utah and the NASPO ValuePoint Cooperative once again for the opportunity to submit our proposal. If you have any questions about our response, please contact me at (703) 246.9360 (ext. 1162), or via e-mail at theresa.grouge@info reliance.com.

Sincerely,



Theresa Grouge
Director of Contracts

3.3.(M) Acknowledgment of Amendments (RFP 5.3)

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.*

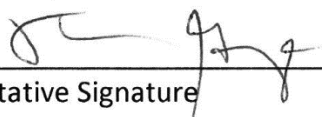
In this section, InfoReliance acknowledges that we have read, reviewed, and understand the totality of Solicitation CH16012 including all addendums, final proposal documents, and answers to questions. We have included our signed acknowledgement forms dated Feb 3 and Feb 10.

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 3, 2016, the amended Attachment A, and the answers to the questions posted by offerors on Bidsync.

By signing below, the Offeror attest to reviewing the documents listed above.

Info Reliance Corporation

Offeror


Representative Signature

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 10, 2016.

By signing below, the Offeror attest to reviewing the documents listed above.

InfoReliance Corporation
Offeror
Representative Signature

3.4.(M) Executive Summary (RFP 5.4)

Excluded from this section per RFP Section 3.12 (para. 3).

This requirement is addressed in **Section 2 Executive Summary**.

3.5.(M) General Requirements for the Service Offerings (RFP 5.5)

In this section, InfoReliance confirms that it will meet and comply with each of the mandatory General Requirements.

3.5.1. Provide a Usage Report Administrator (RFP 5.5.1)

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 in the Master Agreement, and if applicable Participating Addendums.*

If awarded a contract, InfoReliance will assign a Usage Report Administrator who will be responsible for all quarterly sales reporting as described in **Section 42** of the Master Agreement as well as any Participating Addendums. This individual will work under the guidance of the Contract Manager as described in **Section 5.1.3**.

3.5.2. Cooperate with NASPO and SciQuest (RFP 5.5.2)

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 ordering instructions, if awarded a contract.*

InfoReliance will cooperate fully with NASPO ValuePoint, SciQuest, and any authorized agent or successor entity to upload Ordering Instructions to eMarket within thirty (30) days from receipt of written request (per **RFP Section 2.14**). Per Q&A #203, we have also included **Attachment I – Draft Ordering Instructions and Template** as an exhibit to the Master Agreement.

3.5.3. Maintain Completed CSA STAR Registry Self-Assessment (RFP 5.5.3)

RFP 5.5.3: *Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.*

Per Q&A #85, if the CSP (AWS) satisfies this requirement as the manufacturer, the requirement is also satisfied for the reseller (InfoReliance). AWS represents and warrants the accuracy and currency of the information on its completed CAIQ. On behalf of AWS, InfoReliance is submitting

Attachment A – AWS Risk and Compliance Whitepaper. This document includes the completed CAIQ on pages 25-61 as well as detailed mappings to the Cloud Controls Matrix (CCM). This is the latest CAIQ (v3) released by the CSA and covers all IaaS service offerings.

3.5.4. Sample of Service Level Agreement (RFP 5.5.4)

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.

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 the AWS website. For the convenience of reviewers, we have downloaded the following set of SLAs (current as of the time of submission) and provided them as **Attachment B – AWS Sample SLAs**.

AWS Service	AWS SLA Commitment	Courtesy URL
EC2	Monthly Uptime % of at least 99.95%	http://aws.amazon.com/ec2-sla/
S3	Monthly Uptime % of at least 99.9%	http://aws.amazon.com/s3-sla
CloudFront	Monthly Uptime Percentage of at least 99.9%	http://aws.amazon.com/cloudfront/sla/
Route 53	100% Available	http://aws.amazon.com/route53/sla/
RDS	Monthly Uptime Percentage of at least 99.95%	http://aws.amazon.com/rds-sla/

3.6. Recertification of Mandatory Minimums (RFP 5.7)

RFP 5.7: Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the mandatory minimum requirements and technical specifications of the RFP.

If awarded a contract, InfoReliance will annually certify (recertify) that it still meets or exceeds the mandatory minimum requirements and technical specifications for all service offerings.

4. Business Profile

4.1. (M)(E) Business Profile (RFP 6.1)

Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.

Business History and Growth: InfoReliance is a privately held Large Business established in 2000 as a software engineering firm. InfoReliance has delivered more than \$1B in services since inception, with more than \$100M in revenue in each of the last five years. Our Cloud business has grown more than 100% in each of the last three years as our service offerings have expanded to include a wide range of Enterprise IT solutions, a thriving Cybersecurity practice, and Cloud Managed Services along with Software Engineering. Cloud technologies undergird each of these service areas. We deliver Microsoft Office 365 as an enterprise email and productivity solution. We deploy RSA Archer hosted on Amazon Web Services (AWS) for enterprise Governance, Risk Management, and Compliance (eGRC). We deploy ESRI on AWS as a Geographic Information System (GIS). We virtualize software development and test environments on AWS and provide the entire AWS catalog, including IaaS and PaaS, to major federal agencies via Blanket Purchase Agreement (BPA) and Indefinite Delivery Indefinite Quantity (IDIQ) contracts. With this diverse portfolio, InfoReliance is well positioned for continued growth.

Client Base: InfoReliance is primarily a Government contractor, with 60+ customers distributed across Federal Civilian agencies and the Department of Defense (DoD). In recent years, we have expanded into State and Local markets. Notable customers include the City of New York, the South Carolina National Guard (SCNG), the Port of Houston Authority, and the City of Tacoma, WS. We also deliver cloud services to Harvard University, several commercial healthcare providers, and companies such as Amazon.com, Sun Edison, and Battelle.

Number of Employees and Retention Rates: InfoReliance has 340 current employees and retention rates of 92 percent and 90 percent for Cloud Services in the last two years. Within the last three years, we have hired and/or transitioned from elsewhere in the company eight Cloud Architects, Engineers, and Administrators to our core Cloud solutions team, with zero turnover to date. Within the last two years we have hired 30 cloud professionals with AWS and Microsoft cloud solution expertise.

Minimum Three Years Experience Providing Cloud Solutions:

InfoReliance is an AWS Advanced Consulting Partner and in June 2015 became one of the first audited AWS Managed Service Providers. We deployed our first AWS IaaS solution in 2011 at the National Nuclear Security Administration (NNSA) and became an Authorized Reseller in March 2013. We have delivered or are currently delivering cloud services to 30 different customers. This includes large contracts with one or two cloud tasks, small to medium contracts for AWS resale with value-added services, and major multi-million dollar contracts for a broad scope of cloud services. Current AWS customers include:

- ▶ \$55M award from the National Archives and Records Administration for AWS IaaS, PaaS, and Managed Cloud Services
- ▶ Eight year, \$20M award from the Department of Interior (DOI) for ESRI on AWS
- ▶ \$12M Master Agreement with Tennessee Valley Authority (TVA) for AWS IaaS and PaaS, Microsoft Azure, Microsoft Office 365, and cloud consulting services



- ▶ IaaS BPAs for the Federal Bureau of Investigations (FBI) and the Federal Communications Commission (FCC)
- ▶ \$2M AWS Cloud Sandbox for Health and Human Services (HHS)
- ▶ AWS IaaS services to commercial entities (Harvard University, Sun Edison, and Battelle)

InfoReliance has also been a Microsoft Preferred Partner for more than a decade and is a six time Microsoft Partner of the Year. We are a certified Microsoft Cloud Deployment partner, including for Azure and Office 365. Our first multi-million dollar cloud contract was awarded by the Department of Labor (DOL) in February 2013 as a \$49M IDIQ to implement the Office 365 platform and then migrate the entire department from their legacy system. The scope of this IDIQ includes AWS IaaS and PaaS solutions for expanding the DOL enterprise architecture for backup and recovery and then migrating key applications to a cloud hosted environment. In 2014, we were awarded a \$92M BPA from Health and Human Services (HHS) with a similar scope of services. Other Microsoft cloud customers include commercial healthcare providers, the Farm Credit Administration (FCA), the Federal Communications Commission (FCC), and the National Transportation Safety Board (NTSB). For NTSB, we developed a detailed Cloud Roadmap under a \$10M engineering support services BPA and are currently executing a task order for Office 365 implementation and migration.

4.2. (M)(E) 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.

InfoReliance is the only AWS reseller with direct prime contractor experience delivering IT services on multi-million dollar, multiple award contracts with a large pool of purchasing entities. Our primary delivery model for Cloud as well as other IT services has been to establish a BPA or IDIQ with a broad scope of work so that individual buyers within the Government entity can issue task orders or work assignments for their unique requirements. This is a highly flexible and cost-efficient contract structure for the customer, but introduces a much higher degree of complexity for contract management. InfoReliance has consistently received excellent or outstanding ratings for our BPA and IDIQ management as well as our overall program support. Sample customers include the following:

- ▶ **Air Force NETCENTS 2 Application Services (Full and Open):** In May 2015, the Air Force awarded InfoReliance one of several IDIQ contracts with a \$960M ceiling for systems engineering, software development, and application modernization. The Air Force requires all purchasing entities to use the Netcents portfolio of contracts for IT services. Once the Air Force approves an agency-wide cloud adoption strategy, InfoReliance will be providing Air Force customers our full catalog of cloud services from both AWS and Microsoft.
- ▶ **National Nuclear Security Administration (NNSA):** This Alliant Small Business task order includes a base statement of work for the OCIO as well as 20 individual work assignments in support of key Department of Energy initiatives. The total contract value is \$108M to date. From April 2010 to February 2014, InfoReliance was the technical lead for the joint venture and was the only member of the joint venture performing on the contract. Our first cloud project at InfoReliance was to develop a secure collaboration platform hosted on AWS for both classified and unclassified operations across the NNSA enterprise, including more than 25 nuclear sites, plants, and labs around the nation.
- ▶ **White House Executive Office of the President (EOP):** IT Support Services BPA with \$100M ceiling. The scope of work included application development, data migration, cyber security, and enterprise architecture. The contract ended in 2013.

In addition to these representative contracts of similar size, scope, structure, and complexity to this NASPO Master Agreement, our five largest prime contracts for cloud services in the last two years are as follows:

- ▶ **DOL Cloud Email SaaS IDIQ (7 years, \$49M):** In February of 2013, the Department of Labor selected InfoReliance as their primary cloud service partner. The initial task orders focused on discovery and assessment of the existing infrastructure, implementing the Microsoft Office 365 cloud platform, and migrating 18,000 users from the legacy email to Office 365. Subsequent task orders include full service Operations and Maintenance for the Office 365 platform, mobile device management, SharePoint and Skype for Business integration, and deployment of additional cloud IaaS services from AWS to modernize other segments of the DOL enterprise infrastructure. InfoReliance has received Exceptional or Very Good ratings in all categories on the mandatory Contractor Performance Assessment Reports (CPARS) filed by the DOL contracts office.
- ▶ **HHS Email as a Service BPA (5 years, \$92M):** In July of 2014, the Department of Health and Human Services selected InfoReliance for its own agency-wide cloud services contract. HHS intentionally based their procurement model on the InfoReliance contract with DOL, and InfoReliance was selected ahead of much larger systems integrators in part because of successful performance at DOL. While both contracts are based on Microsoft Office 365 and related cloud services, the HHS operating environment is significantly more complex. HHS has more than 120,000 users organized into 11 distinct Operating Divisions. To date InfoReliance has implemented the infrastructure and migrated more than 20,000 users affiliated with the Office of the Chief Information Officer (OCIO). Other large Operating Divisions like the Centers for Disease Control (CDC) and Food and Drug Administration (FDA) are currently preparing additional task orders in accordance with their unique requirements. While they are required to use Office 365, the BPA structure gives them the flexibility to negotiate certain provisions much as a NASPO Participating Entity would negotiate certain terms and conditions for cloud services under a Participating Addendum.
- ▶ **National Aeronautics and Space Administration (NASA) Solutions for Enterprise Procurement (SEWP V) (10 yr GWAC, \$20B ceiling):** NASA is one of three Federal agencies authorized by the Office of Management and Budget (OMB) to establish Government Wide Acquisition Contracts (GWACs). Now in its fifth generation, SEWP is widely used by every agency in the Federal Government to procure everything from printers and laptops to high end servers and enterprise software licenses. Since May of 2015, InfoReliance is a Group A contract holder as the lead partner of a Joint Venture (JV) formed specifically to bid on SEWP V. InfoReliance manages all JV operations, including the Government-facing Program Management Office, and provides our entire AWS catalog of cloud services as well as Microsoft Azure and Office 365 on a managed services model.
- ▶ **National Institutes of Health (NIH) Chief Information Officer Commodities and Solutions (CIO-CS) (10 yr GWAC, \$20B ceiling):** Like NASA, the NIH Information Technology Acquisition and Assessment Center (NITAAC) is authorized by OMB to establish GWACs. NITAAC operates one of the most popular contract vehicles for traditional IT services as well as CIO-CS for “everything IT.” CIO-CS has a similar scope as SEWP V with the same depth and breadth of standard IT commodities, and InfoReliance once again formed a JV with the same three hardware/software companies and was awarded a CIO-CS contract in May of 2015. InfoReliance is the managing partner and sole provider of cloud services within the JV. In September 2015, InfoReliance was awarded a \$55M Flexible Ordering Arrangement (FOA) for managed cloud services from the National Archives and Records Administration (NARA). This is the largest award under CIO-CS to date and includes the full scope of AWS services proposed to NASPO.

- ▶ **Tennessee Valley Authority (TVA) Cloud Services Master Agreement (5 years, \$12M):** TVA is corporate agency of the United States that receives no Federal funding and operates as a financially independent utility provider to more than nine million customers across seven southeastern states. In the summer of 2014, TVA established a Master Agreement with several cloud services providers just as NASPO will establish a Master Agreement with successful bidders on this RFP. TVA has issued several task orders to InfoReliance for on-demand provisioning of AWS services as well as training and consulting services. Future task orders may include an agency wide implementation of AWS infrastructure, migration of legacy systems, and an Office 365 implementation.

4.3.(M) Financials (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.

InfoReliance asserts that we meet the financial strength component of the D&B 3A2 rating (as indicated by Q&A #209, Q&A #237, and Q&A #280). As a privately held firm, we do not publicly provide D&B with the financial information necessary for a 3A2 rating. However, we are submitting our last two years of audited financials to the State of Utah under a Claim of Business Confidentiality along with a letter of reference from our financial institution.

Per RFP 3.12 paragraph 7 and RFP 3.13, we are submitting this confidential information in two separate documents:

- ▶ **Confidential, Protected, or Proprietary Information (Section 7) – Protected Business Confidential.** This includes non-redacted copies of the 2013 and 2014 audited financials and bank letter of reference for evaluation purposes.
- ▶ **Confidential, Protected, or Proprietary Information (Section 7) – Redacted Version.** This includes redacted copies of the 2013 and 2014 audited financials and bank letter of reference for the public record.

4.4.(E) General Information (RFP 6.4)

In this section, we demonstrate that InfoReliance practices and the AWS cloud IaaS offerings exceed the RFP requirements and should be scored **Superior**.

4.4.1. Depth and Breadth of Solutions in Cloud Marketplace (RFP 6.4.1)

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 is the world's leading cloud utility platform and since 2006 has deployed more cloud solutions than all other CSPs combined. Below are some features and benefits of AWS that set our cloud infrastructure services apart as confirmed by Gartner, Inc. in the "2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide" report:

- ▶ **Pace of Innovation:** AWS's pace of innovation is funded and sustained through economies of scale and commitment to delivering the products and services that matter most to customers. The AWS approach to product development and delivery is fundamentally different than that of other Cloud Service Providers (CSPs). AWS teams 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, “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 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 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 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. 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 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 one hour. An elastic infrastructure provides the application with the ability to exploit parallelization in a cost-effective manner reducing time to market.
- ▶ **Cloud Services Automation:** With scriptable infrastructure, 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.

Analyst Reports: The Gartner report that “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.” The Gartner Magic Quadrant for May 2015 **Figure 1** depicts AWS in the Leaders Quadrant.



Figure 1: 2015 Gartner Magic Quadrant for Cloud IaaS. AWS cloud offerings are by far the most mature, complete, and executable among all competitors.

The Forrester Wave report evaluated four of the leading public clouds along 15 key security criteria, detailing the findings about how well each vendor fulfilled their criteria and where they stand in relation to each other. Forrester's evaluation states "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 led with the size of its development and technical support staff as well." **Figure 2** below shows AWS alone among the Leaders.

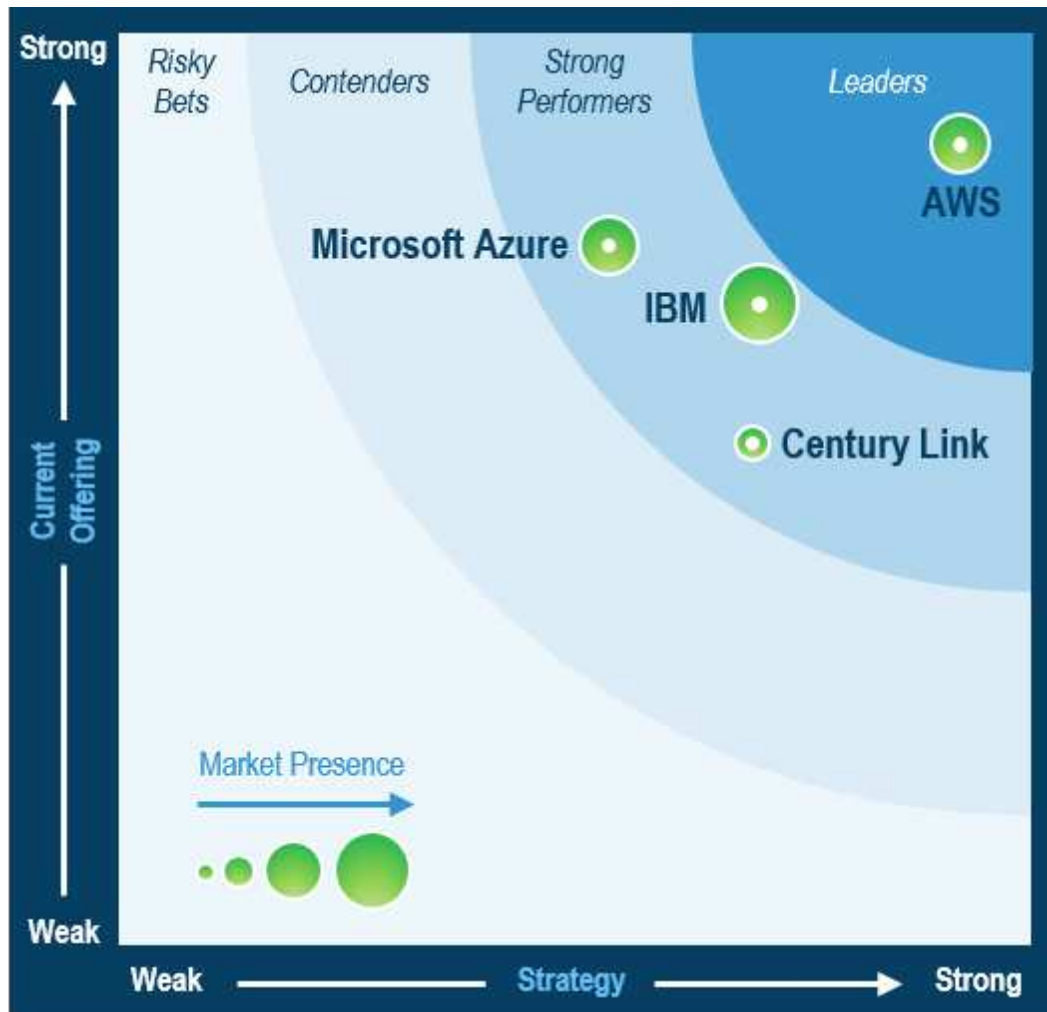


Figure 2: Forrester Wave™ Public Cloud Service Providers' Security, Q4 '14. AWS stands alone among Cloud Service Providers for the Security of its current offerings and future vision.

More analyst reports substantiating the AWS position as the Cloud market leader can be found on the AWS website or readily obtained through industry publications.

4.4.2. Auditing Capabilities and Reports Consistent with SAS 70 (RFP 6.4.2)

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.

InfoReliance's auditing capabilities and reports are consistent with SAS 70 or later. InfoReliance is ISO 20000:27001 certified, has just completed an ISO 9000 audit, holds a Top Secret Facilities clearance, and has successfully achieved FedRAMP ATOs for cloud solutions at multiple cabinet level agencies.

Per Q&A #395, InfoReliance is invoking the full auditing and reporting capabilities of the CSP to satisfy this requirement. 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)

For information on all of the security regulations and standards with which AWS complies, visit the AWS Compliance page.

4.5.(E) Billing and Pricing Practices (RFP 6.5)

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

In this section, InfoReliance demonstrates that our Billing and Pricing practices meet and exceed the RFP requirements and should be scored **Superior**.

We have not included our pricing catalog or any specific cost information in our response to this question. We have included detailed descriptions of practices to demonstrate the complexities of billing and pricing cloud services and the breadth of our expertise.

4.5.1. Billing and Pricing Practices, Including Transparency (6.5.1)

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

InfoReliance maintains a world class AWS cloud billing and pricing framework validated across 30+ cloud engagements and adapted to the specific requirements of GSA Schedule 70 as well as the detailed ordering processes for NASA SEWP V and NITAAC CIO-CS.

AWS Billing Best Practices: InfoReliance Project Accountants are specifically assigned to customers and responsible for invoice preparation, review and submission to the client, processing payments, and collections. Each project accountant is assigned a project and is responsible for accounts receivable and billing tasks related to their assigned project. It is the policy of InfoReliance to generate invoices in an accurate and timely manner based on costs and hours incurred as recorded in the Deltek Costpoint System government approved accounting system. Invoices must be generated in accordance with the terms of our contracts. The billing process includes the following:

Briefing of Contract: The Contract Manager enters the project related information into the accounting system. This includes the customer, contract number, contract type, start date, completion date, contract value, funded value, project labor categories and billing rates. The following data, as applicable, is included in the blue contract file:

- ▶ Contract Brief prepared by the contracts department

- ▶ Copy of the Authorizing document i.e., Contract/Subcontract, Purchase Order, Deliver Order and all modifications
- ▶ Contract correspondence relevant to invoicing
- ▶ Invoice copy of each invoice as submitted to the client
- ▶ Invoice Checklist Review Form/ Invoice Approval form for each invoice
- ▶ Billing and Routing Instructions

Contract Cost Data for Invoicing: Costpoint is the official InfoReliance accounting system. Cost data to support billing is accumulated in the General Ledger, the official cost data source. The Projects module accumulates the cost source data from the general ledger through the Compute Burden Cost process. This contract data is subject to review, validation, and approval by Accounts Payable, the Controller, and the Project Accountant at point of entry and payment in our system. On a monthly basis this data is reviewed by the Controller to ensure accuracy of the cost data. These reviews are evidenced by the Controller's review of monthly PSRs (Project Status Reports). In addition to the point of entry reviews, Project Accountants should expect routine interface with their Program Management teams to communicate any issues identified with cost and hour's information accumulated on the contract. Project Accountants are required to perform their own thorough review of the contract cost accuracy prior to preparing the invoice. The reconciliation of the cost data reported by the Projects Module to data produced in the Billing process is the necessary validation process that ensures a reconciliation of the cost source data to billing. All cost source data is available to the project accountants for use in verifying, validating and reconciling the costs incurred on a particular contract. This is achieved when, at the end of the accounting month or contractually agreed upon invoicing period; the Project Accountant runs the PSR and Revenue Worksheet from the Costpoint Projects Module to confirm that each invoice is prepared accurately and reflects the data recorded in Costpoint. Costs determined to be in error will be resolved prior to billing and only costs that result from timing differences in billing will deviate from the costs recorded in the general ledger. The Project Accountant will do an unbilled reconciliation for all costs that are reflected on the PSR that they are unable to bill and note the reason for the unbilled balance. These unbilled balances are required to be resolved prior to contract close out.

Back-Up Support for Invoicing: Some contracts require that supporting documentation be included in or attached to the invoice. The back-up support may be obtained from multiple sources including the Program Manager, Costpoint reports, Time & Expense module and Accounts Payable records from vendors. In this case, the Project Accountant is responsible for assuring that the required back-up is attached to the invoice and is included in the billing folder.

Invoice Data Validation: It is InfoReliance's policy that one cannot knowingly submit incorrect data on an invoice. Therefore, when it is determined that an error exists, the following apply:

- ▶ The invoice is not submitted until corrections are reflected in Costpoint; or
- ▶ If an invoice is submitted, the incorrect charges will be placed "On Hold" and not be included on the invoice. The Project Accountant will notify the Controller when suspected errors are detected. After the errors have been corrected, the reprinted PSR reports will reflect the approved correcting entries.

Invoice Approval: Project Manager, Controller (and in some cases, Contracts) review and approval of invoices is required prior to the submission of vouchers for payment. An Invoice Checklist Review Form will be prepared by the Project Accountant. The first name of the Project Accountant will be printed legibly on the top of the form, with all entries made in permanent ink. If Project Manager Approval is secured via e-mail, such email will be printed out and attached to the Invoice Approval form. The Controller will sign as the final approver and include the date approved.

Invoice Submission: The approved invoice is submitted to the appropriate client contact according to the contract guidelines.

Real time Billing Access: This is provided to customers through two mechanisms. The first is the **AWS Management Portal**, which is a web application for managing Amazon Web Services. The console provides an intuitive user interface for performing many AWS tasks, including a Billing and Cost Management service which provides features to estimate and plan AWS costs, receive alerts if costs exceed a set threshold, assess the biggest investments in AWS resources and simplify your accounting. The key features are included in the table below:

Key Features	Explanation
Analyzing Costs with Graphs	The AWS Billing and Cost Management console includes the no-cost Cost Explorer tool for viewing AWS cost data as a graph. With Cost Explorer customers can filter graphs by API operations, Availability Zones, AWS service, custom cost allocation tags, Amazon EC2 instance type, purchase options, region, or by linked account. Customers can also see a forecast of future costs, based on your historical cost data.
Budgets	Customers can use budgets to track AWS costs and use the cost visualization provided by Cost Explorer to show the status of budgets and to provide forecasts of estimated costs
Alerts on Cost Limits	Use Amazon CloudWatch to create billing alerts when AWS costs exceed specified thresholds.
AWS Cost and Usage reports	Customers can choose to have AWS publish billing reports to an Amazon Simple Storage Service (Amazon S3) bucket and choose to receive reports that break down costs by the hour or month, by product or product resource, or by defined tags. Customers can view the reports using spreadsheet software such as Microsoft Excel or Apache OpenOffice Calc, or access them from an application using the Amazon S3 API.
Consolidated Billing	The AWS platform is designed to accommodate every size of organization, from small startups to enterprises. If customers set up multiple AWS accounts, they can choose to have each account receive a bill (that is, function as a payer account), or use the Consolidated Billing feature to consolidate multiple linked accounts under one payer account.

The second Real Time Billing Access mechanism is an InfoReliance value added benefit to NASPO customers. The **InfoReliance Advanced Management Portal (iRAMP)** facilitates management and monitoring of cloud assets with full enterprise features for AWS and is extendable to other cloud service providers as needed. iRAMP leverages Windows Identity and integrates seamlessly into existing Active Directory based environments, including those which support Active Directory authentication via Smart Cards, and has a Section 508-compliant modern interface. iRAMP reduces cloud administration costs and manages multiple cloud accounts from a single, centralized interface as shown in **Figure 3**:

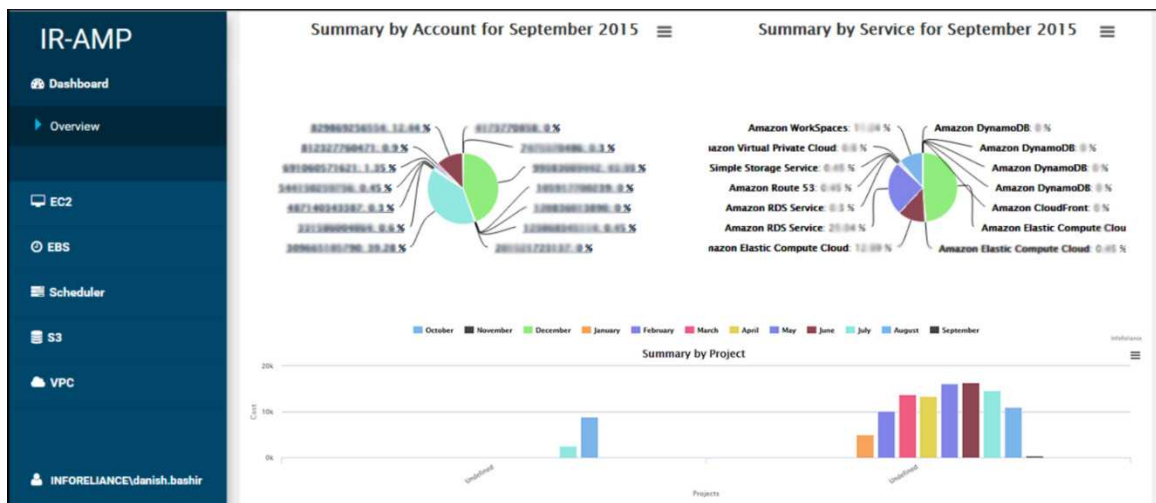


Figure 3: Billing Dashboard. The IR-AMP dashboard shows billing for an organization's multiple AS accounts with breakout of projects for an enterprise view.

AWS Pricing Best Practices: InfoReliance has extensive pricing experience as a strategic AWS partner and reseller on multiple Government contracts. 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%, and relational databases by an average of 28%. **InfoReliance will pass AWS price reductions on to NASPO immediately** by applying the discount structure to real time AWS pricing. The current list rates are published on the AWS website and available in real time through the online pricing calculator. This is a significant advantage over other Government contract models such as GSA Schedule 70 which require substantial lead time and a complete price catalog refresh for modifications and approvals.

AWS Business Support: AWS Business Support is required under the AWS reseller program. For details on the benefits of business support, see **Sections 6.2.1 and 6.3.1B**.

Utility Style Pricing Model: In this model, AWS customers pay only for the resources consumed. AWS's utility-style pricing model is explained in the table below:

Pricing Model	Explanation
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, 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	We continually focus on reducing our data center hardware costs, improving our operational efficiencies, lowering our power consumption, and passing savings back to customers. AWS has reduced prices 51 times since launching in 2006.
Transparency	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 is easy to use and includes video tutorials for first time users. We have provided the publicly accessible URL in our Cost Proposal.
Governance	AWS provides tools to generate detailed and customizable billing reports to meet customer business and compliance needs. Additionally, AWS Partner Network (APN) Consulting Partners can help customers manage and control cost utilization/tracking tools in order to provide customized billing reports.

4.5.2. Typical Cost Impacts (RFP 6.5.2)

RFP 6.5.1: Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

InfoReliance has identified cost impacts and savings that a Purchasing Entity might need to consider with the AWS platform and best practices with AWS to include the following:

- ▶ **Capital expenditure vs Operating Expense:** Using AWS results in a decrease in the need for capital expenditures and a shift to an operating expense budgeting model based on only paying for cloud resources that are consumed.
- ▶ **Software licensing:** AWS offers both bring your own licensing (BYOL) and licensing included models so that customers have the flexibility to use licenses that have already been paid for and purchased through legacy agreements or use an on-demand model based on the AWS services consumed.
- ▶ **On demand vs Reserved instances:** AWS offers customers both on-demand no commitment services and also reserved instance services based on 1 to 3 year commitments and upfront payments. These reserved instances offer a significant discount for customers and also may require alignment with contract periods of performance.

- ▶ **Migration costs:** For customers interested in moving legacy on premise workloads into AWS, there is a cost for the migration services that can be provided either from internal resources or consulting partners like InfoReliance,
- ▶ **Backup costs:** AWS offers highly available cloud services that provide streamlined snapshotting of files and data to other regions and availability zones through automated scripting. This capability may reduce the need for traditional backup tools and processes and result in a cost savings to customers.
- ▶ **Ongoing patching/management:** Just as with on premise workloads and services, AWS requires patching and ongoing system administration services to be performed on a regular basis and these existing costs need to be continued as part of the AWS shared responsibility model with the customer.

4.5.3. NIST Compliant (RFP 6.5.3)

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.

AWS provides NIST compliant cloud infrastructure services. AWS' compliance is validated by two Agency Authorities to Operate (ATOs) achieved based on testing performed against the stringent set of FedRAMP requirements (NIST 800-53 Rev. 4 – Moderate baseline requirements, plus additional FedRAMP security controls). We provide federal security personnel with our security documentation as a means of verifying the security and compliance of AWS in accordance with applicable NIST controls as defined by 800-53 rev4 and the DoD Cloud Computing Security Requirements Guide (SRG). The AWS IaaS platform adheres and is fully compliant to the Essential NIST Characteristics as outlined below:

On-Demand Self Service: AWS provides an on-demand IT infrastructure that lets customers consume only the amount of resources that it actually needs. There are virtually unlimited compute, storage, and bandwidth resources. This will allow customers to provision as many resources as needed without spending on unnecessary services and resources. These resources can be provisioned in Public, Private, or Hybrid cloud deployment models. Most services can also be deployed in Community cloud. AWS IaaS services are provisioned using an On-Demand Self Service model. Customers can provision these services using Management Console, Command Line Interface (CLI) or through an Application Programming Interface (API) as described below.

- ▶ **Management Console:** The AWS Management Console is a single destination for self-managing all customer AWS resources, from EC2 instances to DynamoDB tables. Customers can use the Console to perform any number of tasks, from provisioning a new EC2 instance, provisioning new storage, deploying new applications, or monitoring the health of cloud services without any human interaction with InfoReliance or AWS. The Console enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new IAM Users
- ▶ **Command Line Interface (CLI):** The AWS CLI is a unified tool to self-manage AWS services without any interaction with IR or AWS. With just one tool to download and configure, customers can control multiple AWS services from the command line and automate them through scripts.
- ▶ **Application Programming Interface (API):** AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS API-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits. Customers can use AWS Software Development Kits (SDK) to programmatically provision or manage IaaS without any interaction with IR or AWS.

Broad Network Access: With its 11 Regions across the globe, multiple Availability Zones in each Region, and more than 50 CloudFront (Edge Computing) locations, AWS offers a ubiquitous network access to a broadly distributed user base. Customers can deploy their applications in multiple Regions for low latency, and high availability for great user experience. For security purposes, customers can also use AWS Virtual Private Cloud (VPC) for secure and broad network access. These VPCs can be connected to customers data centers either via Virtual Private Network (VPN), or via AWS Direct Connect. Anywhere a customer has access to the internet, they can log into AWS Management Console to provision or manage any of their AWS services.

Resource Pooling: AWS offers compute, storage, networking and other resources as pooled together to serve multiple cloud customers. IaaS Services are based on a multi-tenant and resource pooling model. Customers can access a pool of AWS servers that function as a single unit without being aware of the physical servers providing the resources. These pooled resources can be deployed in one or more VPCs for public or private cloud deployment models.

Rapid Elasticity: AWS defines elasticity to describe the ability to scale computing resources up and down easily. With its range of services and features, customers can avoid provisioning resources up front for project with variable consumption rate or short lifetimes. The AWS cloud offers customers mechanisms to leverage the elasticity associated with IaaS services through manual or automated mechanism. For manual use of elasticity, for example, customers can provision new instances of virtual machine with a few clicks. Similarly, for the automated use of elasticity of IaaS, customers can use AWS Auto Scaling service. AWS's Auto Scaling helps customers maintain application availability and allows them to scale their Amazon EC2 capacity up or down automatically according to conditions they define. Customers can use Auto Scaling to help ensure that they are running their desired number of Amazon EC2 instances. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. Auto Scaling is well suited both to applications that have stable demand patterns or that experience hourly, daily, or weekly variability in usage.

Measured Service: AWS IaaS Services completely meet this essential characteristics from multiple perspectives. From cost standpoint, AWS provides multiple interfaces including Cost Explorer for looking at the summary of costs and projected costs, to detailed billing using invoices and detailed billing downloadable files. Within the Billing and Cost Management section of the AWS Management Console, customers can enable Cost Explorer, which provides reporting, analytics, and visualization capabilities that customers can use to track and manage their AWS costs. In this same section, customers can also enable Consolidated Billing, which will show overall costs and breakdowns by account. From a services utilization standpoint, IaaS service utilization can be looked at through its CloudWatch Service. With measured service, AWS resources can be monitored, controlled, and reported by users and administrators. For more in-depth monitoring of resources, customers can use Amazon CloudWatch, which allows 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 the customer's applications and services, and any log files their applications generate.

IaaS Deployment Model: The AWS IaaS Service meets the NIST definitions for each of the following deployment models:

- ▶ **Public Cloud:** Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 11 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers'

infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions shown above. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.

- ▶ **Private Cloud:** AWS offers multiple services for private networking, private compute, private storage and private governance. AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Additionally, dedicated instances allow customers to take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that instances will be isolated at the hardware level.
- ▶ **Community Cloud:** Most proposed IaaS Services are also offered in the AWS GovCloud community cloud. AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements.
- ▶ **Hybrid Cloud:** The proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. Customers can seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.

4.6.(E) 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.

InfoReliance is proposing 53 service offerings from our Fulfillment Partner AWS. All of these offerings are classified as IaaS and are available under each of the four NIST deployment models. InfoReliance asserts that these service offerings meet and exceed the requirement for scope and variety of cloud solutions and should be rated **Superior**.

We have provided detailed descriptions of all 53 service offerings in **Section 6.1.1**, including how they satisfy NIST characteristics and deployment model definitions. **Figure 4** below shows the solution subcategories.



Figure 4: Scope and Variety of AWS Cloud Solutions by Subcategory. InfoReliance offers NASPO Participating Entities exceptional depth, breadth, and variety of cloud IaaS solutions.

4.7.(E) 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.

The AWS virtual infrastructure has been designed to provide maximum 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 (TLS).
- ▶ **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. 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 built-in AWS 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.

The sections above describe fully the AWS policies and procedures pertaining to security for cloud delivered services. 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 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. **Figure 5** is a snapshot of the APN partners and categories of products available under the security category in the AWS Marketplace.



Figure 5: AWS Marketplace. The AWS Marketplace provides access to many familiar and trusted security vendors whose solutions can be easily deployed and hosted on AWS.

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 Security Competency Partners can also provide demos and consulting services not available through the AWS Marketplace.

5. Organization Profile

In accordance with the instructions in **RFP Section 3.12 (para. 5)**, this section includes point by point responses to each item described in **RFP Section 7**.

5.1. (M)(E) 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.***

Our Contract Manager will be Ms. Theresa Grouge, who has 23 years experience managing and administering Government contracts and more than five years with contracts for cloud solutions. Ms. Grouge is directly responsible for a \$100M+ annual book of business which includes some of the largest cloud services contracts ever awarded by the Federal Government. Ms. Grouge also manages our GSA IT Schedule 70 and is responsible for all modifications to update and maintain our complete published price catalog of cloud offerings. The Amazon Web Services (AWS) portion of this catalog contains more than 15,000 SKUs and is the same price catalog we are proposing to NASPO. Ms. Grouge is also responsible for our Value Added Reseller agreements and pricing, which includes Microsoft Consulting Services (MCS), Microsoft Premier Support, ESRI ArcGIS, Intel Security (McAfee), and RSA.

Ms. Grouge is the Contract Manager for each of our five largest prime cloud contracts as described in detail in **Section 4.2 Scope of Experience**: DOL Cloud Email SaaS IDIQ (\$49M), HHS EaaS BPA (\$92M), NASA SEWP V GWAC (\$20B ceiling), NITAAC CIO-CS GWAC (\$20B ceiling), and TVA Cloud Services (\$12M). She is also the Contract Manager for several other BPA and IDIQ contracts that include substantial cloud services, such as the Air Force Netcents 2 Application Services (\$960M ceiling), the Department of Justice contract for Microsoft Consulting Services (\$65M), and the NTSB IT Engineering Support Services BPA (\$10M).

5.1.1. Contract Manager Point of Contact and Work Hours (RFP 7.1.1)

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.*

Contract Manager Information	
Name	Ms. Theresa Grouge
Phone	(703) 246.9360 x 1162
Email	theresa.grouge@infoeliance.com
Work Hours	M-F 8:30 AM – 5:30 PM EST

5.1.2. Contract Manager Detailed Experience and Resume (RFP 7.1.2)

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.***

As Director of Contracts for InfoReliance, Ms. Grouge is the final reviewer and signatory authority for all proposals as well as all contract awards, modifications, and funding actions. For each BPA or IDIQ contract, Ms. Grouge personally reviews each task order for statement of work requirements, pricing, terms and conditions, and compliance before submission and again before signing the awarded task order. InfoReliance has delivered more than \$1B in total services since inception in 2000 and more than \$800M of those services and solutions have been on BPA or IDIQ contracts with multiple Purchasing Entities per contract vehicle. Ms. Grouge is directly responsible for our repeated successes in managing these types of contracts and positioning the delivery team for successful performance against requirements. Ms. Grouge is highly regarded by our Microsoft Services customers for her attention to detail and her expertise in the complexities of Microsoft terms and conditions. Her detailed resume follows below:

Ms. Theresa Grouge, NASPO Contract Manager**WORK EXPERIENCE****INFORELIANCE CORP.****2003 – PRESENT**

Director of Contracts: Ms. Grouge manages the Contracts and Pricing departments, and is responsible for the management of all of InfoReliance's government and commercial contracts, including several multi-award and single-award BPAs, IDIQs and GWACs. She is involved in all proposals or quotes for InfoReliance Corporation's \$100M+ annual book of business. Ms. Grouge manages the GSA Schedule 70 contract vehicle including modifications for new Special Item Number (SIN) codes, new manufacturer offerings and administrative modifications. Ms. Grouge is heavily involved in preparing pricing, contractual and subcontracting plan proposal volumes for all major proposal efforts. She responds to task order requests for proposal under the GSA Schedule 70 contract, its BPA contracts, the Navy Seaport-e and NETCENTS 2 MAC IDIQs, the SEWP V and NIH CIO-CS GWACS and commercial contract vehicles.

Ms. Grouge has been instrumental in guiding InfoReliance into new areas of business focus such as value added resale (VAR) business for several manufacturers, including McAfee/Intel, AWS, RSA Archer and Microsoft Corporation services. Ms. Grouge has been the primary program and contract manager for sales and delivery of Microsoft Consulting Services and Microsoft Premier Support services offerings. Ms. Grouge has also managed the state and local government contracts for InfoReliance, including New York City Comptrollers Office, City of Tacoma, New Hanover Regional Medical Center, Public Defenders Service for the District of Columbia, Harvard Business Publishing, President and Fellows of Harvard College, and Port of Houston Authority.

WIPRO CORPORATION**2002 – 2003**

Contracts Manager: Ms. Grouge managed all customer contracts and all prime and subcontractor relationships for the \$35M Global Energy Group (GEG) line of business. She reviewed customer billings, managed collections, and prepared and submitted all proposals. She negotiated and managed Master Services Agreements and all vendor and partner contractual relationships. She assisted with all financial and contractual aspects of the transition before, during, and after American Management Systems sold the GEG business unit to Wipro, including acting as primary interface for all contractual and financial matters for GEG during due diligence.

AMERICAN MANAGEMENT SYSTEMS, INC.**1998 – 2002**

Contracts Manager: Ms. Grouge supported the federal and commercial business units within AMS. Her duties included managing all customer contracts for the Global Energy Group (GEG). She managed all prime and subcontractor relationships for GEG; reviewed customer billings and collections, and was responsible for revenue recognition, financial reporting, and budget development. She prepared and reviewed proposals, drafted task order proposals for Master Services Agreements, supported various federal ID/IQ contracts, and negotiated all vendor and partner contractual relationships for the business unit. She assisted with all financial and contractual aspects of the transition during the sale of the GEG business unit to Wipro, including drafting and negotiating novation agreements and acting as the primary interface during due diligence for both financial and contractual areas of the business unit.

GMSI**1996 – 1998**

Contracts Manager: Ms. Grouge managed the contracts department with a staff of four for a \$20 million federal systems integration company, an 8(a) firm. She produced all major cost and price proposals for federal and commercial customers. She approved all price quotes before they were submitted to the customer, after reviewing them for accuracy and profitability. She developed and implemented standard costing and pricing tools for profit analyses for individual projects and major contracts. She established policies and procedures, both on the department and company

level, to ensure that the departments coordinate and communicate with each other effectively and to improve business processes. She analyzed the company's indirect and direct labor cost structures for cost development and bid purposes. She helped develop the corporate business strategy, as well as strategies for individual proposals and projects. She negotiated contract awards, including major ID/IQ, multiyear contracts.

INTEGRATED SYSTEMS GROUP

1993 – 1996

Contracts Manager: Ms. Grouge managed the contracts department with a staff of six for a \$10 million federal systems integrator and reseller. She generated monthly revenues of over \$100,000 by managing maintenance service contracts. She increased contract profit margins by 5%, on average, by negotiating with vendors and developing new business relationships. She ensured contract compliance, coordinated purchasing and technical service requirements, and acted as the main focal point for negotiations with the customer's procurement and technical personnel on all levels. She participated in senior management meetings to develop corporate strategies and to improve the corporate structure.

EDUCATION

- ▶ MBA, Finance and Marketing, George Mason University, 1995
- ▶ BA, Spanish and Political Science, James Madison University, 1986

5.1.3. Contract Manager Roles and Responsibilities (RFP 7.1.3)

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.

As InfoReliance Director of Contracts and the Contract Manager for the NASPO ValuePoint Master Agreement, Ms. Grouge will be the contractual Point of Contact and sole signatory authority. With the support of her Contracts team and other corporate resources, her specific roles and responsibilities include the following:

- ▶ Negotiate with Participating Entities to establish state-specific terms and conditions for Participating Addendums as well as any optional related services desired by the Participating Entity (as defined in **Section 6.21.2**). The contractual Lead Representative for each Participating Entity will be identified within the executed Participating Addendum.
- ▶ Manage all Contract Actions including modifications to the Master Agreement or individual Participating Addendums, review and execution of individual orders, and modifications to existing orders.
- ▶ Participate in cooperation with the Executive Sponsor in Sales and Marketing functions and expertise, including joint marketing initiatives or sales negotiations with AWS.
- ▶ Respond to all tickets generated by Customer Service Representatives (CSRs) for pricing information, quote requests, order status, and any other issues that fall within their area of responsibility. Per our Draft Ordering Instructions (**Attachment I**), the CSRs will field all phone (toll-free number with call routing) and email (naspo@infoeliance.com) inquiries, create tickets in accordance with our ITIL-based service management process, and assign them to the appropriate organization for resolution.
- ▶ Oversee the maintenance of the complete AWS price catalog as well as all Billing and Pricing practices as defined in **Section 4.5.1**.
- ▶ Engage with project managers and our award-winning AWS architects as needed to develop Level of Effort (LOE) or Rough Order of Magnitude (ROM) estimates for services.
- ▶ Ensure clear handoff to the Cloud Managed Services delivery team, including professional services as defined in **Section 6.21.1**, or optional services as allowed by individual Participating Addendums as defined in **Section 6.21.2**.

- ▶ Serve as the central POC between InfoReliance, AWS as the Cloud Fulfillment Partner, and Purchasing Entities for incident response and escalation for active orders, as described in **Sections 6.3.1A, 6.4.1B and 6.6.8**.
- ▶ Monitor issue resolution in accordance with defined SLAs and order specific performance requirements. Ms. Grouge will oversee lines of communication and escalate as necessary.

Ms. Grouge and her team will interact directly with InfoReliance corporate resources, the InfoReliance Executive Sponsor for NASPO, and the InfoReliance Cloud Managed Services delivery team as demonstrated in **Figure 6**.

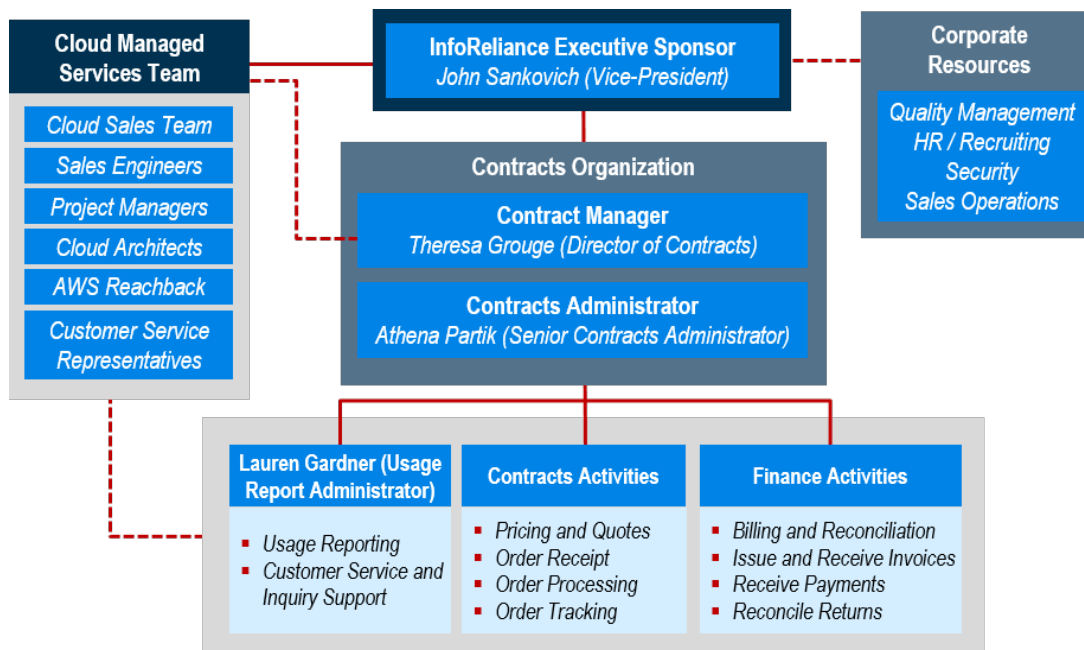


Figure 6: Contracts Organization with Interfaces. Our NASPO Contract Manager will be assisted by a senior Contracts Administrator, a Usage Report Administrator, and other corporate resources to perform all of the contract management activities described in this section.

Ms. Grouge will be closely supported by our Senior Contracts Administrator, Ms. Athena Partik. Ms. Partik has been an AWS pricing specialist for nearly four years and is directly involved in the day to day contract administration of the 30+ projects in our cloud portfolio as well as the quoting, ordering, provisioning, and invoicing of AWS services.

The Contracts Organization is fully staffed for all of the Contracts and Finance activities shown in the org chart and will scale to support additional customers as we execute Participating Addendums. Ms. Grouge and her team will also be supported by other InfoReliance corporate resources to include the ISO-certified and CMMI Level 3-appraised Quality Management practice, Human Resources and Recruiting for staffing and personnel, the Facility Security Officer (FSO), and the Sales Operations team. All interactions with corporate resources as well as the Cloud Managed Services team will follow the same proven model for operations and delivery as on the other large BPA, IDIQ, and GWAC contract vehicles.

Finally, our Usage Report Administrator will be Ms. Lauren Gardner. Ms. Gardner currently supports our GWAC/IDIQ Program Management Office with contracts administration, technical refreshes, quoting, ordering, and reporting including contract access fees. She will work under the direction of Ms. Grouge to complete all of the activities defined in **Section 42** of the Master Agreement in accordance with existing processes to ensure accurate and timely reporting.

6. Technical Response

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable. If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

The following sections provide the required point-by-point responses to all of the Technical Requirements as outlined in **RFP Section 8**. InfoReliance has specifically partnered with AWS for this NASPO proposal based on the AWS leading platform over other CSP platforms. In particular, and as recognized by Gartner and every analyst report, AWS is the #1 cloud utility platform in the world and offers the following key additional attributes that will be of value to NASPO states members:

Why AWS for IaaS?	
Strength	Proof
Flexible	AWS enables organizations to retain existing programming models, operating systems, databases, and architectures. This flexibility helps organizations mix and match architectures according to business needs.
Cost Effective	With AWS, organizations pay only for what they use, without upfront 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 cost.
Innovative	In 2015 alone, AWS launched 722 new services and features. Through continuous innovation, AWS gives customers access to leading edge technologies and the most efficient infrastructure without costly recapitalization investments.
Secure	AWS builds services in accordance with security best practices, provides the appropriate security features in those services, and documents how to use those features. This ensures end-to-end security and privacy.
Experience	Organizations who use AWS leverage many years of experience delivering secure, reliable infrastructure at a large scale.
Breadth and Depth	The world's most robust set of core cloud infrastructure services for compute, storage, database, network, and security.
AWS Pace of Innovation	AWS continually expands its services to support virtually any cloud workload and now has more than 50 services that range from compute, storage, networking, database, analytics, application services, deployment, management and mobile. In 2015, AWS launched 722 new features and/or services for a total of 1,896 since inception in 2006.
Open Source Focus	AWS fully embraces open source as a companion to AWS's strategic business model—and Linux, Xen, MySQL and other open source projects remain the core technologies behind AWS. As an example of this open source commitment, since 2011 Red Hat and AWS have teamed to offer Red Hat Enterprise Linux (RHEL) on Amazon EC2.
Managed Database Choices	Amazon Relational Database Service (Amazon RDS) is a fully managed relational database service. RDS provides the leading database engines to choose from – including Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB. AWS also offers Amazon Aurora, an AWS 3 year R&D effort that provides a MySQL-compatible, relational database engine that combines the speed and availability of high-end commercial databases (Oracle) with the simplicity and cost-effectiveness of open source databases. Amazon Aurora provides up to five times better performance than MySQL at a price point one tenth that of a commercial database while delivering similar performance and availability.
Online Software Marketplace	The AWS Marketplace is an online software store that helps customers find, buy, and immediately start using the software and services that has been specifically configured and tested to run in the EC2 cloud. It's the largest cloud online marketplace for software tools in the world and has pioneered purchasing enterprise software by the hour and pay for what you use model.

6.1.(M)(E) Technical Requirements (RFP 8.1)

In this section, InfoReliance demonstrates that our cloud service offerings meet or exceed the technical requirements and should be scored **Superior**.

6.1.1. Cloud Service Models and Deployment Models (RFP 8.1.1)

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**.

InfoReliance is proposing 53 distinct AWS offerings under the IaaS Service Model as defined by NIST. We are not providing any SaaS or PaaS offerings at this time. Each of the proposed services is fully compliant with the NIST essential characteristics as described in **Section 6.1.2** below. In the following sections, we have provided tables with the following for each offering:

- ▶ Brief description of the IaaS Offering and how it meets the IaaS Service Model requirements
- ▶ How it meets the requirements for each of the four Deployment Models
- ▶ Courtesy URLs to the AWS product description and product documentation

InfoReliance understands that evaluators may be reviewing printed copies and not able to access URLs. All necessary information for scoring the technical proposal is contained in the text of the tables. However, we strongly encourage Participating Entities to consider these URLs when making their best value determinations before establishing a Participating Addendum. AWS provides extensive service descriptions including product details, features and benefits, FAQs, developer resources, product documentation, release notes, video demonstrations, and more.

6.1.1.1. IaaS Offering: Amazon EC2

IaaS Offering: Amazon EC2	
Description of IaaS Offering	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon's data centers—that you use to build and host your software systems.
How it Meets Service Model Requirements	The Amazon EC2 offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in RFP Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Additionally, dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.

IaaS Offering: Amazon EC2	
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers IT compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon EC2 Product Documentation: http://aws.amazon.com/documentation/ec2/

6.1.1.2. IaaS Offering: Amazon EC2 Container Service

IaaS Offering: Amazon EC2 Container Service	
Description of IaaS Offering	Amazon EC2 Container Service is a highly scalable, high- performance container management service that supports Docker containers and allows you to easily run distributed applications on a managed cluster of Amazon EC2 instances.
How it Meets Service Model Requirements	The Amazon EC2 Container Service offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in

IaaS Offering: Amazon EC2 Container Service	
	Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon EC2 Container Service Product Documentation: http://aws.amazon.com/ecs/faqs/

6.1.1.3. IaaS Offering: AWS Lambda

IaaS Offering: AWS Lambda	
Description of IaaS Offering	AWS Lambda is a compute service that runs your code in response to events and automatically manages the compute resources for you, making it easy to build applications that respond quickly to new information. AWS Lambda starts running your code within milliseconds of an event such as an image upload, in-app activity, website click, or output from a connected device.
How it Meets Service Model Requirements	The AWS Lambda offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual

IaaS Offering: AWS Lambda	
	network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Lambda Product Documentation: http://aws.amazon.com/documentation/lambda/

6.1.1.4. IaaS Offering: Auto Scaling

IaaS Offering: Auto Scaling	
Description of IaaS Offering	Auto Scaling is a web service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks.
How it Meets Service Model Requirements	The Auto Scaling offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation

IaaS Offering: Auto Scaling	
	at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Auto Scaling Product Documentation: http://aws.amazon.com/documentation/autoscaling/

6.1.1.5. IaaS Offering: Elastic Load Balancing

IaaS Offering: Elastic Load Balancing	
Description of IaaS Offering	Elastic Load Balancing automatically distributes your incoming application traffic across multiple Amazon EC2 instances. It detects unhealthy instances and reroutes traffic to healthy instances until the unhealthy instances have been restored. Elastic Load Balancing automatically scales its request handling capacity in response to incoming traffic.
How it Meets Service Model Requirements	The Elastic Load Balancing offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.

IaaS Offering: Elastic Load Balancing	
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Elastic Load Balancing Product Documentation: http://aws.amazon.com/documentation/elasticloadbalancing/

6.1.1.6. IaaS Offering: Amazon VPC

IaaS Offering: Amazon VPC	
Description of IaaS Offering	Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
How it Meets Service Model Requirements	The Amazon VPC offering allows the customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications.

IaaS Offering: Amazon VPC	
	This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For the customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private networking, Amazon VPC lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon VPC Product Documentation: http://aws.amazon.com/documentation/vpc/

6.1.1.7. IaaS Offering: Amazon Route 53

IaaS Offering: Amazon Route 53	
Description of IaaS Offering	Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service.
How it Meets Service Model Requirements	The Route 53 offering allows the customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications.

IaaS Offering: Amazon Route 53	
	This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For the customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private networking, Route 53 lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Route 53 Product Documentation: http://aws.amazon.com/documentation/route53/

6.1.1.8. IaaS Offering: AWS Direct Connect

IaaS Offering: AWS Direct Connect	
Description of IaaS Offering	AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 GB or 10 GB Ethernet fiber optic cable. One end of the cable is connected to your router and the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly

IaaS Offering: AWS Direct Connect	
	to the AWS cloud and Amazon VPC, bypassing Internet service providers in your network path.
How it Meets Service Model Requirements	The AWS Direct Connect offering allows the customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For the customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private networking, AWS Direct Connect lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Direct Connect Product Documentation: http://aws.amazon.com/documentation/directconnect/

6.1.1.9. IaaS Offering: Amazon S3

IaaS Offering: Amazon S3	
Description of IaaS Offering	Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data, at any time, from anywhere on the web. You can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console.
How it Meets Service Model Requirements	The Amazon S3 offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon S3 Product Documentation: http://aws.amazon.com/documentation/s3/

6.1.1.10. IaaS Offering: Amazon Glacier

IaaS Offering: Amazon Glacier	
Description of IaaS Offering	Amazon Glacier is a storage service optimized for infrequently used data, or “cold data.” The service provides secure, durable, and extremely low-cost storage for data archiving and backup. With Amazon Glacier, you can store your data cost effectively for months, years, or even decades. Amazon Glacier enables you to offload the administrative burdens of operating and scaling storage to AWS, so you do not have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations.
How it Meets Service Model Requirements	The Amazon Glacier offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity’s control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers’ infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers’ existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.

IaaS Offering: Amazon Glacier

Courtesy URLs	Product Description: Amazon Glacier Product Documentation: http://aws.amazon.com/documentation/glacier/

6.1.1.11. IaaS Offering: Amazon EBS

IaaS Offering: Amazon EBS

Description of IaaS Offering	Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance. With Amazon EBS, you only pay for what you use.
How it Meets Service Model Requirements	The Amazon EBS offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS

IaaS Offering: Amazon EBS	
	IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLS	Product Description: Amazon EBS Product Documentation: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

6.1.1.12. IaaS Offering: Amazon CloudFront

IaaS Offering: Amazon CloudFront	
Description of IaaS Offering	Amazon CloudFront is a content delivery web service. It integrates with other AWS cloud services to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no commitments.
How it Meets Service Model Requirements	The CloudFront offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend

IaaS Offering: Amazon CloudFront	
	their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLS	Product Description: Amazon CloudFront Product Documentation: http://aws.amazon.com/documentation/cloudfront/

6.1.1.13. IaaS Offering: AWS Import/Export

IaaS Offering: AWS Import/Export	
Description of IaaS Offering	AWS Import/Export accelerates transferring large amounts of data between the cloud and portable storage devices that you mail to us. AWS transfers data directly onto and off of your storage devices using Amazon's high-speed internal network. Your data load typically begins the next business day after your storage device arrives at AWS. After the data export or import completes, we return your storage device. For large data sets, AWS Import/Export is significantly faster than Internet transfer and more cost effective than upgrading your connectivity.
How it Meets Service Model Requirements	The AWS Import/Export offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.

How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Import/Export Product Documentation: http://aws.amazon.com/documentation/importexport/

6.1.1.14. IaaS Offering: AWS Storage Gateway

IaaS Offering: AWS Storage Gateway	
Description of IaaS Offering	AWS Storage Gateway is a service that connects an on premises software appliance with cloud-based storage to provide seamless and secure integration between your on premises IT environment and AWS's storage infrastructure.
How it Meets Service Model Requirements	The AWS Storage Gateway offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across

IaaS Offering: AWS Storage Gateway	
	multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Storage Gateway Product Documentation: http://aws.amazon.com/documentation/storagegateway/

6.1.1.15. IaaS Offering: Amazon RDS

IaaS Offering: Amazon RDS	
Description of IaaS Offering	Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks. Database engines available through Amazon RDS include Amazon Aurora, MySQL, Oracle, Microsoft SQL Server, and PostgreSQL.
How it Meets Service Model Requirements	The Amazon RDS offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private database and storage, AWS provides a wide assortment of private storage options. Amazon RDS can be hosted in a private subnet in a VPC of a Purchasing Entity's choice. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.

IaaS Offering: Amazon RDS	
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon RDS Product Documentation: http://aws.amazon.com/documentation/rds/

6.1.1.16. IaaS Offering: Amazon DynamoDB

IaaS Offering: Amazon DynamoDB	
Description of IaaS Offering	Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. You can use Amazon DynamoDB to create a database table that can store and retrieve any amount of data, and serve any level of request traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified by the customer and the amount of data stored, while maintaining consistent and fast performance.
How it Meets Service Model Requirements	The Amazon DynamoDB offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private database and storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.

IaaS Offering: Amazon DynamoDB	
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon DynamoDB Product Documentation: http://aws.amazon.com/documentation/dynamodb/

6.1.1.17. IaaS Offering: Amazon Redshift

IaaS Offering: Amazon Redshift	
Description of IaaS Offering	Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse solution that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. You can start small with no commitments and scale to a petabyte or more.
How it Meets Service Model Requirements	The Redshift offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private database and storage, AWS provides a wide assortment of private options. Amazon RedShift, for example, can be limited to a VPC of a Purchasing Entity's choice as well as in a private subnet to keep it private. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-

IaaS Offering: Amazon Redshift	
	side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Redshift Product Documentation: http://aws.amazon.com/documentation/redshift/

6.1.1.18. IaaS Offering: Amazon ElastiCache

IaaS Offering: Amazon ElastiCache	
Description of IaaS Offering	Amazon ElastiCache is a web service that makes it easy to set up, manage, and scale distributed, in-memory cache environments in the cloud. It provides a high-performance, resizable, and cost-effective in-memory cache, while removing the complexity associated with deploying and managing a distributed cache environment.
How it Meets Service Model Requirements	The ElastiCache offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private database and storage, AWS provides a wide assortment of private options. Amazon ElastiCache, for example, can be limited to a VPC

IaaS Offering: Amazon ElastiCache	
	of a Purchasing Entity's choice as well as in a private subnet to keep its nodes private. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon ElastiCache Product Documentation: http://aws.amazon.com/documentation/elasticache/

6.1.1.19. IaaS Offering: Amazon EMR

IaaS Offering: Amazon EMR	
Description of IaaS Offering	Amazon Elastic MapReduce (Amazon EMR) is a web service that makes it easy to process large amounts of data efficiently. Amazon EMR uses Hadoop processing combined with several AWS products to perform such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing.
How it Meets Service Model Requirements	The Amazon EMR offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications.

IaaS Offering: Amazon EMR	
	This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For analytics services, AWS provides a wide assortment of private options. Amazon EMR, for example, can have its nodes limited to a VPC of a Purchasing Entity's choice as well as in a private subnet to keep it private. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon EMR Product Documentation: http://aws.amazon.com/documentation/elasticmapreduce/

6.1.1.20. IaaS Offering: Amazon Kinesis

IaaS Offering: Amazon Kinesis	
Description of IaaS Offering	Amazon Kinesis is a managed service that scales elastically for real-time processing of streaming big data. The service takes in large streams of data records that can then be consumed in real time by multiple data processing

IaaS Offering: Amazon Kinesis	
	applications that can be run on Amazon EC2 instances. The data processing applications use the Amazon Kinesis Client Library and are called “Amazon Kinesis applications.”
How it Meets Service Model Requirements	The Amazon Kinesis offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity’s control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers’ infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers’ existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Kinesis Product Documentation: http://aws.amazon.com/documentation/kinesis/

6.1.1.21. IaaS Offering: AWS Data Pipeline

IaaS Offering: AWS Data Pipeline	
Description of IaaS Offering	AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services as well as on premises data sources at specified intervals. With AWS Data Pipeline, you can regularly access your data where it's stored, transform and process it at scale, and efficiently transfer the results to AWS cloud services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR.
How it Meets Service Model Requirements	The AWS Data Pipeline offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private deployments, AWS Data Pipeline can be limited to use only those nodes that are private to a Purchasing Entity. These nodes can be in a private subnet in a VPC that belongs to a Purchasing Entity's account. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing

IaaS Offering: AWS Data Pipeline	
	infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Data Pipeline Product Documentation: http://aws.amazon.com/documentation/data-pipeline/

6.1.1.22. IaaS Offering: Amazon Mobile Analytics

IaaS Offering: Amazon Mobile Analytics	
Description of IaaS Offering	Amazon Mobile Analytics is a service that lets you easily collect, visualize, and understand application usage data at scale. Many mobile application analytics solutions deliver usage data several hours after the events occur. Amazon Mobile Analytics is designed to deliver usage reports within 60 minutes of receiving data from an application so that you can act on the data more quickly.
How it Meets Service Model Requirements	The Amazon Mobile Analytics offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For analytics services, AWS provides a wide assortment of private options. Amazon Mobile Analytics, for example, can have its nodes limited to a VPC of a Purchasing Entity's choice as well as in a private subnet to keep it private. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private

IaaS Offering: Amazon Mobile Analytics	
	networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Mobile Analytics Product Documentation: http://aws.amazon.com/documentation/mobileanalytics/

6.1.1.23. IaaS Offering: AWS Identity & Access Management

IaaS Offering: AWS Identity & Access Management	
Description of IaaS Offering	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.
How it Meets Service Model Requirements	The Identity & Access Management offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private administration, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it

IaaS Offering: AWS Identity & Access Management	
	compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Identity & Access Management Product Documentation: http://aws.amazon.com/documentation/iam/

6.1.1.24. IaaS Offering: AWS Directory Service

IaaS Offering: AWS Directory Service	
Description of IaaS Offering	AWS Directory Service is a managed service that allows you to connect your AWS resources with an existing on premises Microsoft Active Directory or to set up a new, stand-alone directory in the AWS cloud. Connecting to an on premises directory is easy, and once this connection is established, all users can access AWS resources and applications with their existing corporate credentials.
How it Meets Service Model Requirements	The AWS Directory Service offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements.

IaaS Offering: AWS Directory Service	
	This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Directory Service Product Documentation: http://aws.amazon.com/documentation/directory-service/

6.1.1.25. IaaS Offering: AWS Service Catalog

IaaS Offering: AWS Service Catalog	
Description of IaaS Offering	AWS Service Catalog is a service that allows administrators to create and manage approved catalogs of resources that end users can then access via a personalized portal. You can control which users have access to which applications or AWS resources to enable compliance with your business policies, while users can easily browse and launch products from the catalogs you create.
How it Meets Service Model Requirements	The AWS Service Catalog offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual

IaaS Offering: AWS Service Catalog	
	network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Service Catalog Product Documentation: http://aws.amazon.com/servicecatalog/

6.1.1.26. IaaS Offering: AWS Config

IaaS Offering: AWS Config	
Description of IaaS Offering	AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.
How it Meets Service Model Requirements	The AWS Config offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.

IaaS Offering: AWS Config	
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Config Product Documentation: http://aws.amazon.com/documentation/config/

6.1.1.27. IaaS Offering: AWS CloudHSM

IaaS Offering: AWS CloudHSM	
Description of IaaS Offering	AWS CloudHSM provides secure cryptographic key storage to customers by making Hardware Security Modules (HSMs) available in the AWS cloud.
How it Meets Service Model Requirements	The AWS CloudHSM offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where

IaaS Offering: AWS CloudHSM	
	anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private administration AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS CloudHSM Product Documentation: http://aws.amazon.com/documentation/cloudhsm/

6.1.1.28. IaaS Offering: AWS Key Management Service

IaaS Offering: AWS Key Management Service	
Description of IaaS Offering	AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS KMS is integrated with other AWS cloud services including Amazon EBS, Amazon S3, and Amazon Redshift. AWS KMS is also

IaaS Offering: AWS Key Management Service	
	integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
How it Meets Service Model Requirements	The AWS Key Management offering allows the NASPO customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO customers control.
How it meets Private Cloud Deployment Model Requirements	For the NASPO workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private key management, AWS allows NASPO to implement fine-grained access roles and groups for every workload. Depending on NASPO needs, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. The proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	The proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Key Management Service Product Documentation: http://aws.amazon.com/documentation/kms/

6.1.1.29. IaaS Offering: AWS CloudTrail

IaaS Offering: AWS CloudTrail	
Description of IaaS Offering	With AWS CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS Software Development Kits (SDKs), the command line tools, and higher-level AWS cloud services. You can also identify which users and accounts called AWS APIs for services that support AWS CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate AWS CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn AWS CloudTrail logging on and off.
How it Meets Service Model Requirements	The AWS CloudTrail offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing

IaaS Offering: AWS CloudTrail	
	infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS CloudTrail Product Documentation: http://aws.amazon.com/documentation/cloudtrail/

6.1.1.30. IaaS Offering: Amazon CloudWatch

IaaS Offering: Amazon CloudWatch	
Description of IaaS Offering	Amazon CloudWatch is a web service that enables you to collect, view, and analyze metrics. Amazon CloudWatch lets you programmatically retrieve your monitoring data, view graphs, and set alarms to help you troubleshoot, spot trends, and take automated action based on the state of your cloud environment.
How it Meets Service Model Requirements	The Amazon CloudWatch offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. For private monitoring, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private

IaaS Offering: Amazon CloudWatch	
	networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon CloudWatch Product Documentation: http://aws.amazon.com/documentation/cloudwatch/

6.1.1.31. IaaS Offering: AWS Management Console

IaaS Offering: AWS Management Console	
Description of IaaS Offering	Access and manage Amazon cloud services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on-the-go.
How it Meets Service Model Requirements	The AWS Management Console offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS Management Console can be leveraged to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Command Line Interface lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.

IaaS Offering: AWS Management Console	
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Management Console Product Documentation: http://aws.amazon.com/console/faqs/

6.1.1.32. IaaS Offering: AWS Command Line Interface

IaaS Offering: AWS Command Line Interface	
Description of IaaS Offering	The AWS Command Line Interface (CLI) is a unified tool used to manage your AWS cloud services. With just one tool to download and configure, you can control multiple AWS cloud services from the command line and automate them through scripts.
How it Meets Service Model Requirements	The AWS Command Line Interface offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS CLI can be leverage to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and

IaaS Offering: AWS Command Line Interface	
	password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Command Line Interface lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Command Line Interface Product Documentation: http://aws.amazon.com/documentation/cli/

6.1.1.33. IaaS Offering: APIs

IaaS Offering: APIs	
Description of IaaS Offering	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.
How it Meets Service Model Requirements	The AWS APIs Interface offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS APIs can be leveraged to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Command Line Interface lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend

IaaS Offering: APIs	
	customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: APIs Product Documentation: https://aws.amazon.com/tools/

6.1.1.34. IaaS Offering: AWS Elastic Beanstalk

IaaS Offering: AWS Elastic Beanstalk	
Description of IaaS Offering	With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and AWS Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.
How it Meets Service Model Requirements	The AWS Elastic Beanstalk offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS Elastic Beanstalk can be leverage to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Command Line Interface lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon

IaaS Offering: AWS Elastic Beanstalk	
	Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Elastic Beanstalk Product Documentation: http://aws.amazon.com/documentation/elasticbeanstalk/

6.1.1.35. IaaS Offering: AWS CloudFormation

IaaS Offering: AWS CloudFormation	
Description of IaaS Offering	AWS CloudFormation gives developers and system administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application.
How it Meets Service Model Requirements	The AWS CloudFormation offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.

IaaS Offering: AWS CloudFormation	
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS CloudFormation can be leverage to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, CloudFormation lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS

IaaS Offering: AWS CloudFormation	
	IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLS	Product Description: AWS CloudFormation Product Documentation: http://aws.amazon.com/documentation/cloudformation/

6.1.1.36. IaaS Offering: AWS CodeDeploy

IaaS Offering: AWS CodeDeploy	
Description of IaaS Offering	AWS CodeDeploy is a service that automates code deployments to Amazon EC2 instances. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one Amazon EC2 instance or thousands.
How it Meets Service Model Requirements	The AWS CodeDeploy offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS CodeDeploy can be leverage to deploy code in any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, CodeDeploy lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.

IaaS Offering: AWS CodeDeploy	
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS CodeDeploy Product Documentation: http://aws.amazon.com/documentation/codedeploy/

6.1.1.37. IaaS Offering: AWS CodeCommit

IaaS Offering: AWS CodeCommit	
Description of IaaS Offering	AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. AWS CodeCommit eliminates the need for you to operate your own source control system or worry about scaling its infrastructure. You can use AWS CodeCommit to store anything from code to binaries, and it supports the standard functionality of Git, allowing it to work seamlessly with your existing Git-based tools.
How it Meets Service Model Requirements	The AWS CodeCommit offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS CodeCommit can be leverage to build any private cloud deployments including private compute, private network, and private storage.

IaaS Offering: AWS CodeCommit	
	For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, CodeCommit lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.

IaaS Offering: AWS CodeCommit**Courtesy URLs****Product Description:** [AWS CodeCommit](#)**Product Documentation:** <http://aws.amazon.com/codecommit/>**6.1.1.38. IaaS Offering: AWS CodePipeline****IaaS Offering: AWS CodePipeline****Description of IaaS Offering**

AWS CodePipeline is a continuous delivery and release automation service that aids smooth deployments. You can design your development workflow for checking in code, building the code, deploying your application into staging, testing it, and releasing it to production. You can integrate third-party tools into any step of your release process or you can use AWS CodePipeline as an end-to-end solution.

How it Meets Service Model Requirements

The AWS CodePipeline offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.

How it meets Private Cloud Deployment Model Requirements

For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS CodePipeline can be leveraged to build any private cloud deployments including private compute, private network, and private storage.

For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level.

For private networking, CodePipeline lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.

For private *storage*, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.

How it Meets Community Cloud Deployment Model Requirements

AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements.

IaaS Offering: AWS CodePipeline	
	This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS CodePipeline Product Documentation: http://aws.amazon.com/codepipeline/

6.1.1.39. IaaS Offering: AWS OpsWorks

IaaS Offering: AWS OpsWorks	
Description of IaaS Offering	AWS OpsWorks provides a simple and flexible way to create and manage stacks and applications. With AWS OpsWorks, you can provision AWS resources, manage their configuration, deploy applications to those resources, and monitor their health.
How it Meets Service Model Requirements	The AWS OpsWorks offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS OpsWorks can be leverage to build any private cloud deployments including private compute, private network, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual

IaaS Offering: AWS OpsWorks	
	network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, OpsWorks lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS OpsWorks Product Documentation: http://aws.amazon.com/documentation/opsworks/

6.1.1.40. IaaS Offering: Amazon WorkDocs

IaaS Offering: Amazon WorkDocs	
Description of IaaS Offering	Amazon WorkDocs is a fully managed, secure enterprise storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity. Users can comment on files, send them to others for feedback, and upload new versions without having to resort to emailing multiple versions of their files as attachments.
How it Meets Service Model Requirements	The AWS WorkDocs offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon WorkDocs can be leveraged to work with any private cloud deployments including compute, network, and storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, WorkDocs lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible

IaaS Offering: Amazon WorkDocs	
	fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon WorkDocs Product Documentation: http://aws.amazon.com/documentation/workdocs/

6.1.1.41. IaaS Offering: Amazon Workspaces

IaaS Offering: Amazon Workspaces	
Description of IaaS Offering	Amazon WorkSpaces is a fully managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow end users to access the documents, applications, and resources they need with the device of their choice, including laptops, iPad, Kindle Fire, or Android tablets. With a few clicks in the AWS Management Console, customers can provision a high-quality cloud desktop experience for any number of users at a cost that is highly competitive with traditional desktops and half the cost of most Virtual Desktop Infrastructure (VDI) solutions
How it Meets Service Model Requirements	The AWS Workspaces offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. A Purchasing Entity can integrate AWS WorkSpaces with an existing Active Directory by using the AD Connector feature. To enable integration a Participating Entity needs to ensure that their domain is reachable via an Amazon Virtual Private Cloud VPC (this could mean that Active Directory domain controllers for a Participating Entity domain are running on Amazon EC2 instances, or that they are reachable via a VPN connection and are located in a Participating Entity's on-premises network). A Participating Entity can provide configuration information to the WorkSpaces service such as DNS server IP addresses, domain names, and an account with sufficient permissions to create computer accounts in a Participating Entity's Active Directory domain. Once a Participating Entity has configured this integration, when they launch a Workspace, they can select which users to provide a

IaaS Offering: Amazon Workspaces	
	WorkSpace to from a list of users in their domain. When the WorkSpaces for these users are launched, the WorkSpaces will join a Participating Entity's Active Directory domain, and the users will be able to connect to them using their existing Active Directory credentials. For private storage, AWS provides a wide assortment of private storage options. Amazon WorkDocs provides capabilities to provide private document storage to Amazon WorkSpaces. Similarly, Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Workspaces Product Documentation: http://aws.amazon.com/documentation/workspaces/

6.1.1.42. IaaS Offering: Amazon AppStream

IaaS Offering: Amazon AppStream	
Description of IaaS Offering	The Amazon AppStream web service deploys your application on AWS infrastructure and streams input and output between your application and devices such as personal computers, tablets, and mobile phones. Your application's processing occurs in the cloud, so it can scale to handle vast

IaaS Offering: Amazon AppStream	
	computational loads. Devices need only display output and return user input, so the client application on the device can be lightweight in terms of file size and processing requirements.
How it Meets Service Model Requirements	The Amazon AppStream offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon AppStream can be used in a private cloud deployment setting including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, AppStream lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across

IaaS Offering: Amazon AppStream	
	multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon AppStream Product Documentation: http://aws.amazon.com/documentation/appstream/

6.1.1.43. IaaS Offering: Amazon CloudSearch

IaaS Offering: Amazon CloudSearch	
Description of IaaS Offering	Amazon CloudSearch is a fully managed service in the cloud that makes it easy to set up, manage, and scale a search solution for your website. Amazon CloudSearch enables you to search large collections of data such as web pages, document files, forum posts, or product information. With Amazon CloudSearch, you can quickly add search capabilities to your website without having to become a search expert or worry about hardware provisioning, setup, and maintenance. As your volume of data and traffic fluctuates, Amazon CloudSearch automatically scales to meet your needs.
How it Meets Service Model Requirements	The Amazon CloudSearch offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon CloudSearch can be used in a private cloud deployment that includes private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, CloudSearch lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables

IaaS Offering: Amazon CloudSearch	
	and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon CloudSearch Product Documentation: http://aws.amazon.com/documentation/cloudsearch/

6.1.1.44. IaaS Offering: Amazon SWF

IaaS Offering: Amazon SWF	
Description of IaaS Offering	Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is performed by a component of your application. Coordinating tasks across the application involves managing inter-task dependencies, scheduling, and concurrency in accordance with the logical flow of the application. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying

IaaS Offering: Amazon SWF	
	about underlying complexities such as tracking their progress and maintaining their state.
How it Meets Service Model Requirements	The Amazon SWF offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon SWF can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, EMR lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.

IaaS Offering: Amazon SWF	
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon SWF Product Documentation: http://aws.amazon.com/documentation/swf/

6.1.1.45. IaaS Offering: Amazon SQS

IaaS Offering: Amazon SQS	
Description of IaaS Offering	Amazon Simple Queue Service (Amazon SQS) is a messaging queue service that handles messages or workflows between other components in a system.
How it Meets Service Model Requirements	The Amazon SQS offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon SQS can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, SQS lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.

IaaS Offering: Amazon SQS	
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon SQS Product Documentation: http://aws.amazon.com/documentation/sqs/

6.1.1.46. IaaS Offering: Amazon SES

IaaS Offering: Amazon SES	
Description of IaaS Offering	Amazon Simple Email Service (Amazon SES) is an outbound-only email-sending service that provides an easy, cost-effective way for you to send email.
How it Meets Service Model Requirements	The Amazon SES offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon SES can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of

IaaS Offering: Amazon SES	
	the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, SES lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon SES Product Documentation: http://aws.amazon.com/documentation/ses/

6.1.1.47. IaaS Offering: Amazon SNS

IaaS Offering: Amazon SNS	
Description of IaaS Offering	Amazon Simple Notification Service (Amazon SNS) is a web service that enables applications, end users, and devices to instantly send and receive notifications from the cloud.
How it Meets Service Model Requirements	The Amazon SNS offering allows customers to provision compute, storage, and network processing at multiple levels that can be leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon SNS can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, SNS lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across

IaaS Offering: Amazon SNS	
	multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon SNS Product Documentation: http://aws.amazon.com/documentation/sns/

6.1.1.48. IaaS Offering: Amazon Elastic Transcoder

IaaS Offering: Amazon Elastic Transcoder	
Description of IaaS Offering	Amazon Elastic Transcoder lets you convert media files that you have stored in Amazon S3 into media files in the formats required by consumer playback devices. For example, you can convert large, high-quality digital media files into formats that users can play back on mobile devices, tablets, web browsers, and connected televisions.
How it Meets Service Model Requirements	The Amazon Elastic Transcoder offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon Elastic Transcoder can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Elastic Transcoder lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC.

IaaS Offering: Amazon Elastic Transcoder	
	For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon Elastic Transcoder Product Documentation: http://aws.amazon.com/documentation/elastictranscoder/

6.1.1.49. IaaS Offering: Amazon Cognito

IaaS Offering: Amazon Cognito	
Description of IaaS Offering	Amazon Cognito is a simple user identity and data synchronization service that helps you securely manage and synchronize application data for your users across their mobile devices. You can create unique identities for your users through a number of public login providers (Amazon, Facebook, and Google) and also support unauthenticated guests.
How it Meets Service Model Requirements	The Amazon Cognito offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where

IaaS Offering: Amazon Cognito	
	anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon Cognito can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, Cognito lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend

IaaS Offering: Amazon Cognito	
	their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLS	Product Description: Amazon Cognito Product Documentation: http://aws.amazon.com/cognito/dev-resources/

6.1.1.50. IaaS Offering: Amazon FPS

IaaS Offering: Amazon FPS	
Description of IaaS Offering	Amazon Flexible Payments Service facilitates the digital transfer of money between any two entities, humans or computers.
How it Meets Service Model Requirements	The Amazon FPS offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon FPS can be used with a private cloud deployment including private compute, private networking, and private storage. For private compute, AWS allows the customer to implement fine-grained access roles and groups for every workload. Depending on the needs of the Participating Entity, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level. Dedicated Instances let NASPO take full advantage of the benefits of Amazon VPC and the AWS cloud – on-demand elastic provisioning; pay only for what you use; and a private, isolated virtual network, all while ensuring that NASPO Amazon EC2 compute instances will be isolated at the hardware level. For private networking, FPS lets the NASPO Participating Entity provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a defined virtual network. Customers will have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Customers can easily customize the network configuration for their Amazon VPC. For private storage, AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest. Additionally, Amazon Elastic Block Store (EBS) supports encrypted file systems for EC2 instances and can be made single-tenant with EC2 Dedicated Instances.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements.

IaaS Offering: Amazon FPS	
	This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: Amazon FPS Product Documentation: https://payments.amazon.com/developer

6.1.1.51. IaaS Offering: AWS Support

IaaS Offering: AWS Support	
Description of IaaS Offering	AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers to help customers of all sizes and technical abilities successfully utilize the products and features provided by AWS.
How it Meets Service Model Requirements	The AWS Support offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. Amazon Support can be used with a private cloud deployment including private compute, private networking, and private storage.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.

IaaS Offering: AWS Support	
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Support Product Documentation: https://aws.amazon.com/documentation/aws-support/

6.1.1.52. IaaS Offering: AWS Trusted Advisor

IaaS Offering: AWS Trusted Advisor	
Description of IaaS Offering	AWS Trusted Advisor acts like your customized cloud expert, and it helps you provision your resources by following best practices. AWS Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps. Since 2013, customers have viewed over 1.7 million best-practice recommendations, many leading directly to substantial cost reductions.
How it Meets Service Model Requirements	The AWS Trusted Advisor offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. AWS Trusted Advisor can be used with a private cloud deployment including private compute, private networking, and private storage
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed IaaS Service is also offered in the AWS GovCloud community cloud.

IaaS Offering: AWS Trusted Advisor	
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Trusted Advisor Product Documentation: https://aws.amazon.com/premiumsupport/faqs/

6.1.1.53. IaaS Offering: AWS Marketplace

IaaS Offering: AWS Marketplace	
Description of IaaS Offering	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.
How it Meets Service Model Requirements	The AWS Marketplace offering allows customers to provision compute, storage, and network processing at multiple levels that can leveraged to deploy any arbitrary software including OS and other software applications. This aligns closely to the NIST Service Models as described in Attachments C and D. The underlying cloud infrastructure is managed by AWS, where anything above the OS is completely in the NASPO Participating Entity's control.
How it meets Private Cloud Deployment Model Requirements	For customer workloads, AWS offers multiple services for private networking, private compute, private storage and private governance. A Purchasing Entity can leverage any of the AWS Marketplace offerings in a private cloud deployment as well.
How it Meets Community Cloud Deployment Model Requirements	AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. This proposed service is currently not offered in the AWS GovCloud community, but if there is demand from customer then it can be added to the AWS GovCloud roadmap.
How it Meets Public Cloud Deployment Model Requirements	Any of the AWS services offered under IaaS can be deployed in a public cloud offered by AWS. AWS is divided into 12 global regions. Regions provide the top level of redundancy, durability, and availability. Each region

IaaS Offering: AWS Marketplace	
	is completely independent of other regions, providing the greatest possible fault tolerance and stability for customers' infrastructure. AWS offers it compute, storage, network, application, analytics, managements and many other services in all of the Regions. These services can be combined across multiple Regions and Availability Zones for critical and highly available workloads.
How it Meets Hybrid Cloud Deployment Model Requirements	This proposed IaaS Service offers the most integrated networking, security and access controls, data integration and life-cycle management, and resource and deployment management capabilities to make hybrid architecture successful. For example, the proposed IaaS Service can extend customers on premise network configuration into their own virtual private networks on the AWS Cloud. AWS IaaS services will operate as if they are part of customers' existing corporate network. Customers can also extend their physical connectivity, which provides dedicated, consistent, private networking between their data center and the AWS regions of choice. AWS IaaS Services allow customers to seamlessly integrate their existing infrastructure with the elastic, scalable resources available in the AWS Cloud. Integrated networking services include VPC, and Direct Connect.
Courtesy URLs	Product Description: AWS Marketplace Product Documentation: https://aws.amazon.com/marketplace/help/

6.1.2. How Solutions Meet NIST Essential Characteristics (RFP 8.1.2)

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 these characteristics as defined in NIST Special Publication 800-145:

AWS IaaS offerings fully comply with all five essential cloud computing characteristics. As defined in NIST Special Publication 800-145 and as shown in **Figure 7** below.

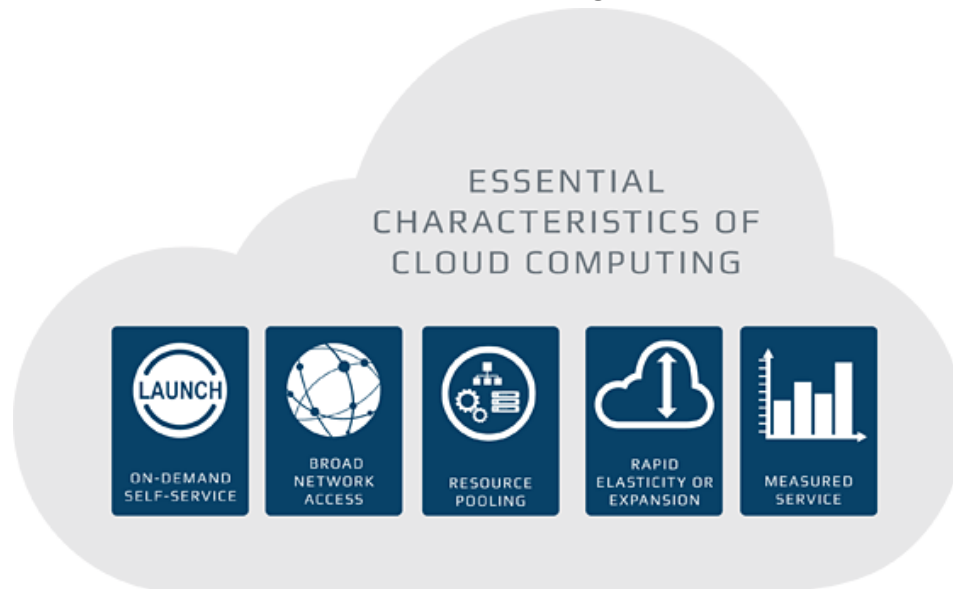


Figure 7: NIST Cloud Essential Characteristics: AWS meets all of the 5 Essential Characteristics of Cloud Computing as defined by NIST.

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

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.

AWS supports on-demand deployment of AWS services 24x7x365. The NIST on-demand self service capability is met by AWS through the AWS Management Console—a web application for

managing Amazon Web Services. The console provides an intuitive user interface for performing many AWS tasks. This includes working with Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting Amazon CloudWatch alarms, and more. Customers can access each service from the AWS Management Console, which also provides information about accounts and billing.

To access any AWS Service on-demand in the console, click **Services** located at the top of the page. A full dropdown list of available AWS services will appear, as shown in **Figure 8**.

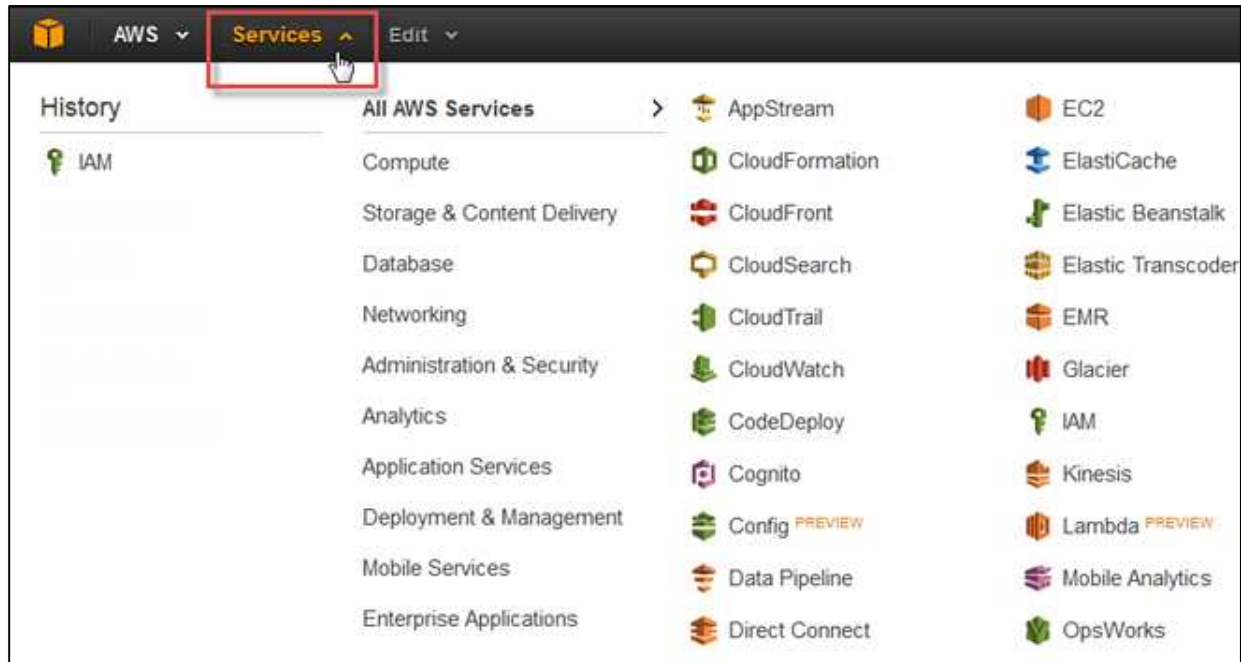


Figure 8: AWS Management Console. How to Access the Full List of Services.

To search for a list of available services within a specific category, such as **Compute & Networking**, hover over the category and click a service name to open the console for that service and use the AWS NIST compliant, on-demand, self-service Management Console (**Figure 9**).



Figure 9: AWS Management Console. How to Access a List of Available Services in a Category.

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

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. As the CSP, AWS owns and maintains the network-connected hardware required for these application services, while customers provision and use what they need via an AWS web application, mobile client, or a set of published and well documented APIs. Specific NIST compliant network access services provided by AWS include the following:

- ▶ **Amazon Virtual Private Cloud (VPC):** VPC enables customers to launch Amazon Web Services (AWS) resources into a virtual network that has been defined. This virtual network closely resembles a traditional network in a customer own data center, with the benefits of using the scalable infrastructure of AWS.
- ▶ **AWS Direct Connect:** Direct Connect links an internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to a router, the other to an AWS Direct Connect router. With this connection in place, customers can create virtual interfaces directly to the AWS cloud and Amazon Virtual Private Cloud, bypassing Internet service providers in a network path.
- ▶ **AWS Elastic Load Balancing (ELB):** ELB automatically distributes incoming application traffic across multiple Amazon EC2 instances. It detects unhealthy instances and reroutes traffic to healthy instances until the unhealthy instances have been restored. Elastic Load Balancing automatically scales its request handling capacity in response to incoming traffic.
- ▶ **Amazon Route 53 Documentation:** Route 53 is a highly available and scalable Domain Name System (DNS) web service.

6.1.2.3. NIST Characteristic – Resource Pooling (RFP 8.1.2.3)

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.

AWS services meet the NIST requirement for resource pooling by allowing physical and logical devices of the same resource group to be dynamically attached and separated as needed to meet service demand. As an example of AWS resource pooling, the AWS ECS compute service can ensure that the number of Amazon EC2 instances being utilized scales up seamlessly by adding more resources in the pool during demand spikes to maintain performance, and scales down automatically and removes resources from the pool during demand lulls to minimize costs.

6.1.2.4. NIST Characteristic – Rapid Elasticity (RFP 8.1.2.4)

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 meets the NIST requirement for rapid elasticity through the AWS services of Elastic Load Balancing and Auto Scaling. These can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases. Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It detects unhealthy instances and reroutes traffic to healthy instances until the unhealthy instances have been restored. Elastic Load Balancing automatically scales its request handling capacity in response to incoming traffic. Auto Scaling is a web service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks.

6.1.2.5. NIST Characteristic – Measured Service (RFP 8.1.2.5)

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.

AWS meets the NIST requirement for measured service and allows customers to pay only for the resources that are actually consumed, like instance-hours or data transfer. For example, AWS EC2 compute service customers will be charged at the end of each month for EC2 resources actually consumed. If the customer launches 20 small instances at some point in time, the instances will begin booting immediately, but will not necessarily all start at the same moment.

Each instance will store its actual launch time and the customer will only be charged for its hours of execution at the beginning of each hour relative to the time it launched. Each instance will run until one of the following occurs: a customer terminates the instance, the instance shuts itself down, or the host terminates.

6.1.3. Solution Subcategories (RFP 8.1.3)

RFP 8.1.3: Offeror must identify for each Solution the subcategories that it offers for each service model.

InfoReliance offers the following subcategories of IaaS services from AWS (**Figure 10**).



Figure 10: AWS Services and Solution Subcategories. InfoReliance offers NASPO Participating Entities exceptional depth, breadth, and variety of cloud IaaS solutions.

6.1.4. Willingness to Comply With Attachments C & D (RFP 8.1.4)

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**.

InfoReliance confirms its willingness to fully comply with **Attachments C & D**.

6.1.5. Adherence to Attachment D, Scope of Services (RFP 8.1.5)

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**.

InfoReliance certifies that it agrees to adhere to the services, definitions, and deployment models identified in **Attachment D, Scope of Services**, during the term of the contract. This is supported by our completed **Attachment H – InfoReliance Identification of Service Models**. In that document, we certifies that for all 53 IaaS Service Offerings, AWS is capable of storing and securing data at all three risk levels as defined by FIPS PUB 199 (Low Risk Data, Moderate Risk Data, High Risk Data). The US East and US West regions hold a Provisional Authorization for level 2 which permits mission owners to deploy public, unclassified information in these regions with both the AWS Authorization and the mission application's ATO. The AWS GovCloud (US) region now holds a Provisional Authorization for levels 2 and 4 and permits mission owners to deploy the full range of controlled, unclassified information categories covered by these levels.

6.2. (E) Subcontractors (RFP 8.2)

In this section, we certify that InfoReliance and its Fulfillment Partner AWS meet or exceed NASPO's requirements for cloud solutions and services and should be scored **Superior**. InfoReliance and AWS have a long-standing relationship with InfoReliance as a systems integrator and AWS as the Cloud Service Provider, with an extensive history of exceptional joint performance. Our formal relationship is documented in **Attachment C – AWS Letter of Support**.



6.2.1. Detailed Plans for Providing Services (RFP 8.2.1)

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.

All IaaS services will be provided directly by InfoReliance based on our authorized reseller agreement with our Fulfillment Partner Amazon Web Services (AWS). All Value Added Services will be performed directly by InfoReliance without the use of subcontractors, as described in **Section 6.21**. The table below outlines specific roles for both InfoReliance and AWS support.

InfoReliance Customer Support	AWS Business Support
■ Contract Customer Service – easy to use email, web, and phone 12x5 for contract support (see Section 6.4). ■ Quickly and efficiently get answers to billing and account inquiries via a designated senior customer service AWS accredited professional who is familiar the account. ■ Support for InfoReliance Required and Optional Value Added Services as described in Section 6.21.	■ Technical and Incident Support 24x7 and access to AWS Cloud Support Engineers via email, chat, & phone ■ Trusted Advisor – Full Checks - Access to the full set of Trusted Advisor checks and guidance to provision your resources following best practices to help reduce cost, increase performance and fault tolerance, and improve security. ■ Architecture Support – Business – Contextual guidance on how services fit together to meet your specific use-case, workload, or application. ■ AWS Support API - Programmatic access to AWS Support Center features to create, manage, and close your support cases,

InfoReliance Customer Support	AWS Business Support
Use as an alternative request process to Contract manager and Executive sponsor—also available via direct communication processes.	and operationally manage your Trusted Advisor check requests and status. Third Party Software Support - Guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

In some cases, customers may also require AWS Enterprise Support which includes the same features as Business Support but also offers:

- **Technical Account Manager:** Designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices, and proactively keep AWS environment operationally healthy.
- **Infrastructure Event Management:** Architecture and scaling guidance, and real-time operational support during the preparation and execution of planned events, product launches, and migrations.

6.2.2. Subcontractors to Perform Contract Requirements (RFP 8.2.2)

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.

All IaaS services will be provided directly by InfoReliance based on our authorized reseller agreement with our Fulfillment Partner Amazon Web Services. InfoReliance will perform all Value Added Services directly and without the use of subcontractors, as described in **Section 6.21**.

6.2.3. Subcontractor Qualifications (RFP 8.2.3)

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.

All IaaS services will be provided directly by InfoReliance based on our authorized reseller agreement with our Fulfillment Partner Amazon Web Services. AWS is the undisputed leader among CSPs according to industry studies (see **Section 4.4.1**) and is exceptionally well-qualified in all its service offerings and practices. All Value Added Services will be performed directly by InfoReliance without the use of subcontractors, as described in **Section 6.21**.

6.3.(E) Working with Purchasing Entities (RFP 8.3)

In this section, we demonstrate that our processes and approach to working with Purchasing Entities meet and exceed the RFP requirements and should be scored **Superior**.

6.3.1. Working with Purchasing Entities (RFP 8.3.1)

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.

AWS has deployed some of the world's most advanced security for global cloud architecture and combined this with both physical and operational security processes. In the event of a data breach, AWS provides world class Incident Response before, during, and after an incident. The AWS Incident Management team employs industry-standard diagnostic procedures during business-impacting events and staff operators provide 24x7x365 coverage.

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, methods of communication, and management commitment. It has been developed in alignment with ISO 27001 standards with system utilities appropriately restricted and monitored. The AWS incident management program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance. AWS maintains and updates incident response playbooks to reflect emerging risks and lessons learned from past incidents. Plans are tested and updated through the due course of business (at least monthly). This incident response process includes a three-phased approach:

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 uses early indicator alarms to proactively identify potential issues.
 - ▶ **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.
2. **Recovery Phase:** Relevant resolvers will conduct root cause analysis. Once troubleshooting, break/fix, and affected components are addressed, the call leader will assign next steps including follow-up documentation and actions to complete 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.

A. Personnel (Including Contract Manager) Involved at Various Stages

Personnel	Commitment
AWS Executives	Members of the Senior Executive management team, Security Team, and the Audit Committee of the Board of Directors review the AWS services security resiliency plans regularly and in the event of any AWS security and data breach.
InfoReliance Executives	Review of all Incidents and immediate point of Customer escalation for all issues and current status.
InfoReliance Contract Manager and Security Team	The Contract Manager serves as the central point of contact for customers for incident response and escalation as described in Section 6.6.8 . She is supported by a Security and Compliance manager assigned to the customer.
AWS incident response team and support desk	Provide Incident resolution and 24x7 support
InfoReliance response team and support desk	Customers will maintain control and root access to their AWS systems and direct communication with AWS support. InfoReliance will support this process and facilitate resolution activities.

B. Response Times

AWS Business Support	AWS Enterprise Support
Case Severity & Response Times Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours	Case Severity & Response Times Critical: < 15 minutes Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours

C. Processes and Timelines

During an incident, a customer may open an unlimited number of requests for support through an unlimited number of customer contacts. AWS utilizes an ITIL based service delivery model to resolve incidents based on the response timelines and a commitment to customer security as outlined in this section.

D. Methods of Communication and Assistance

AWS has also 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. Technical Support is provided with 24x7 access to senior Cloud and Security Support Engineers via email, chat, and phone. 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 security and compliance details about AWS.

E. Other Information Vital to Understanding the Service Provided

AWS has documented many of the security architecture and compliance features in the AWS Risk and Compliance Whitepaper. This has been attached as **Attachment A** for NASPO's review as part of our response to the CSA STAR requirements.

6.3.2. Adware, Unauthorized Software, and Unauthorized Marketing (RFP 8.3.2)

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.

InfoReliance will neither engage in or permit its agents to push adware, software, or marketing not explicitly authorized by the Purchasing Entity. 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. Application Hosting Environments (RFP 8.3.3)

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

AWS offers application-hosting environments that fully support a user test/staging environment that is identical to production. AWS offers a diverse set of services that can be leveraged to build multiple application environments including development, testing, staging and production. For example, with AWS CloudFormation templates, developers can create application stacks for any environment including production environment. The same CloudFormation stack then can be used to create other test/staging environments identical to production environment.

6.3.4. Accessibility Policies (RFP 8.3.4)

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.

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

6.3.5. Applications Accessible Using Multiple Browser Platforms (RFP 8.3.5)

RFP 8.3.5: Offeror must describe whether or not its applications and content delivered through Web browsers are accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

AWS supports the following browser platforms and meets all RFP requirements:

Browser	Version	Service
Google Chrome	Latest 3 Versions	All services
Mozilla Firefox	Latest 3 Versions	All services
Microsoft Internet Explorer	11, 10, 9	All services
Microsoft Edge	12	All services
Apple Safari	9, 8, 7, 6	All services

6.3.6. Meeting with the Purchasing Entity (RFP 8.3.6)

RFP 8.3.6: Offeror must describe how it will, prior to the execution of an SLA, 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.

InfoReliance 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. AWS defines all customer data as “Your Content” and that customers own all right, title, and interest in and to Your Content.

6.3.7. Project Schedule and Work Plans (RFP 8.3.7)

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

InfoReliance uses our proven iFRAME project management framework to develop schedules and work plans for solution implementation. **Figure 11** below shows a nominal project plan.

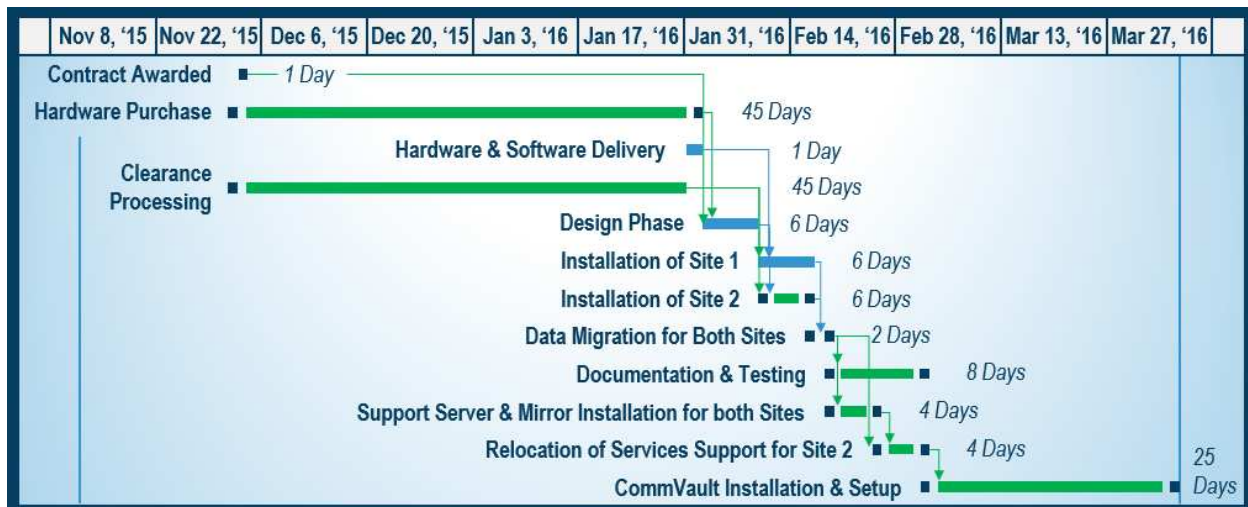


Figure 11: Representative Project Plan. InfoReliance manages, monitors, and audits all projects in accordance with our CMMI Level 3-assessed quality management and solution delivery framework.

6.4.(E) Customer Service (RFP 8.4)

In this section, we demonstrate that our Customer Service capabilities meet or exceed RFP requirements and should be scored **Superior**.

6.4.1. Ensuring Excellent Customer Service

RFP 8.4.1: Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include: a) Quality assurance measures b) Escalation plan; and c) Service Level Agreement (SLA).

A. Quality Assurance Measures

InfoReliance delivers comprehensive cloud solutions through the iFRAME solution delivery framework, which is assessed at CMMI Level 3 and incorporates PMI/PMBOK, ISO 20000:27001, and ITIL quality management standards as shown in **Figure 12**.

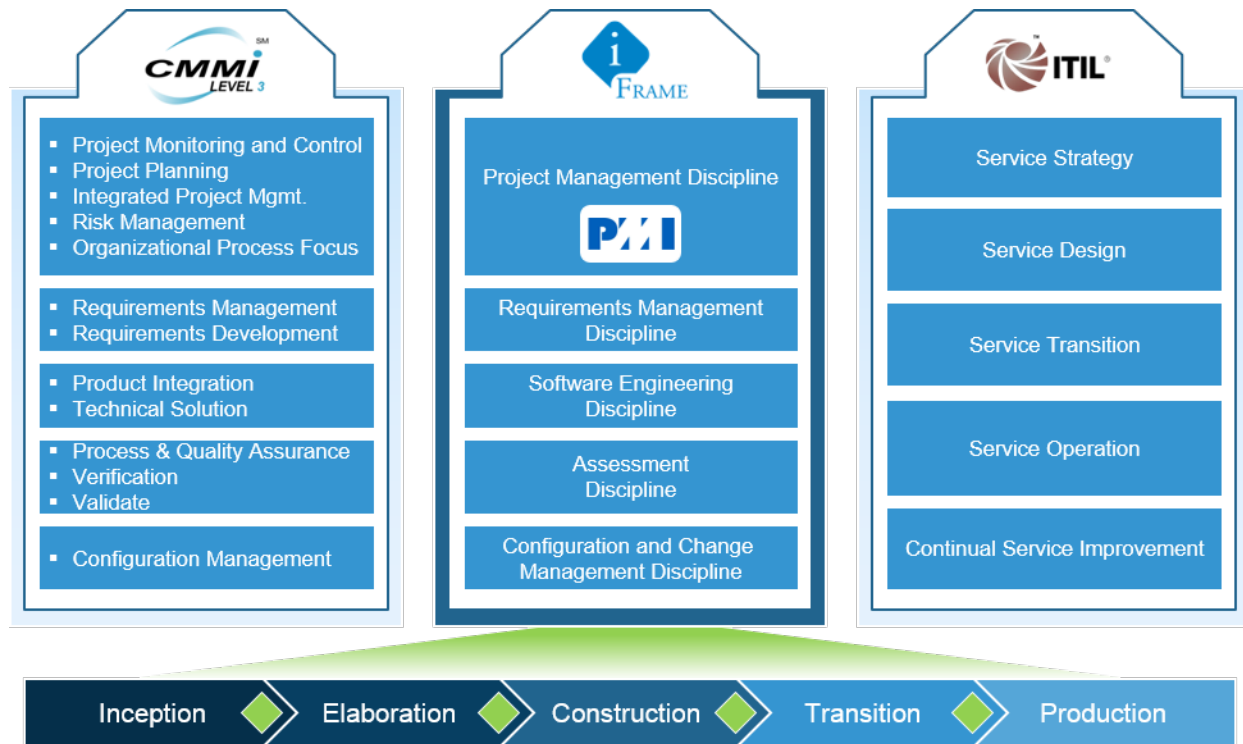


Figure 12: Solution Delivery Framework iFRAME integrates proven practices and industry certifications to manage all projects and solutions in accordance with established quality standards.

B. Escalation Plan

Customers will have a single point of contact with the Contract Manager and will have immediate access to the InfoReliance Executive Sponsor. For individual projects, the Technical Lead will report directly to the Contracts Manager and be responsible for the successful delivery of technical program services. Direct AWS support will be available, as needed, in addition to the InfoReliance professional corporate reach back services. The entire team will have immediate access to corporate reach back in the areas of Quality, Contracts, Billing, and Security. Each area will be contained within a quality framework focused on continuous improvement.

C. Service Level Agreement (SLA)

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 the AWS website. For the convenience of reviewers, we have downloaded the following set of SLAs (current as of the time of submission) and provided them as **Attachment B – AWS Sample SLAs**. We have also provided the URLs as a courtesy.

AWS Service	SLA Commitment	Courtesy URL
EC2	Monthly Uptime % of at least 99.95%	http://aws.amazon.com/ec2-sla/
S3	Monthly Uptime % of at least 99.9%	http://aws.amazon.com/s3-sla
CloudFront	Monthly Uptime Percentage of at least 99.9%	http://aws.amazon.com/cloudfront/sla/
Route 53	100% Available	http://aws.amazon.com/route53/sla/
RDS	Monthly Uptime Percentage of at least 99.95%	http://aws.amazon.com/rds-sla/

InfoReliance will provide SLAs for value added services at the order level based on requirements and services requested. For Customer Service, our SLA commitment exceeds the minimum requirements of RFP 8.4.2, paragraphs B and C, as described in the following section.

6.4.2. Ability to Comply with Customer Service Requirements (RFP 8.4.2)

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.

A. Lead Representatives

The InfoReliance Contract Manager will be the single point of contact for the NASPO ValuePoint Master Agreement. The contractual Lead Representative for each Participating Entity will be identified within the executed Participating Addendum. Customer Service Representatives will also be assigned as leads for each Participating Entity that executes an Addendum, with backup assignments as necessary to maintain coverage in accordance with our ITIL Services Management framework for Enterprise Service Desk.

B. Customer Service Representative(s) Availability

InfoReliance CSRs will be available by phone (toll free) during Federal Government schedule and regular business hours (M-F 7AM to 7PM) and 24x7x365 via web portal and email. AWS Business Support is available 24x7 via email, chat, and phone.

C. Customer Service Representative(s) Responsiveness within One Business Day

InfoReliance CSR leads will be AWS certified and will be able to resolve most inquiries related to InfoReliance value-added services at first contact. This includes inquiries for sales, quoting, ordering, account provisioning, billing and invoicing, and training. AWS Business Support is required as part of the AWS Reseller program and provides direct technical support and incident response from AWS Cloud Support Engineers 24x7 via email, chat, and phone. As detailed in **Section 6.2.1**, AWS Business Support is in addition to InfoReliance Customer Support and provides direct access to technical expertise for specific service offerings.

D. Design Services for Applicable Categories

InfoReliance offers a world class and industry leading set of both Required and Optional Value added Services to include design services as described in **Section 6.21**.

E. Installation Services for Applicable Categories

InfoReliance offers a world class and industry leading set of both Required and Optional Value added Services to include design services as described in **Section 6.21**.

6.5.(E) Security of Information (RFP 8.5)

In this section, we demonstrate that our approach to Information Security meets and exceeds the RFP requirements and should be scored **Superior**.

6.5.1. Agreements to Protect Data (RFP 8.5.1)

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.

Within AWS, Customers always maintain full ownership and control of their data during the entire technology lifecycle. This is based on the following 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.

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. Detailed data disposal procedures, policies, and destruction confirmation process are addressed in **Section 6.11 Data Disposal**.

6.5.2. Data Privacy and Security (RFP 8.5.2)

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

InfoReliance and AWS will not have access to any customer data and will comply with all applicable laws related to data privacy and security.

6.5.3. Conditions to Access User Accounts or Data (RFP 8.5.3)

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.*

InfoReliance and AWS will not have access to any customer data and therefore cannot access a Purchasing Entity's user accounts or data unless specifically provided access by the customer. Neither InfoReliance nor AWS will request access except in 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.

6.6.(E) Privacy and Security (RFP 8.6)

In this section, we demonstrate that our capabilities meet and exceed the RFP requirements for Privacy and Security and should be scored **Superior**.

6.6.1. NIST Compliance (RFP 8.6.1)

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.*

AWS adheres to NIST definitions for cloud essential characteristics, service model, and deployment models, and all AWS services comply with those definitions. Even in future, any new AWS services and features will also comply with these NIST definitions as they related to the Scope of Services described in RFP Attachment D. AWS can support all types of data with its offered services. With its compliance with many industry standards, it can cover public as well as private data including PII and HIPAA data.

InfoReliance and AWS confirm our 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 RFP Attachment D, including supporting the different types of data that NASPO Purchasing Entities may provide.

6.6.2. Security Certifications (RFP 8.6.2)

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.*

InfoReliance holds the following certifications:

- ▶ ISO 20000:27001
- ▶ ISO 9000 (in process with audit completed as of this submission)
- ▶ Top Secret Facilities Clearance

Per Q&A #395, InfoReliance is relying on additional certifications from the CSP. 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)

AWS is a FedRAMP Compliant Cloud Service Provider (CSP) and thus allows customers and partners to leverage AWS as an Infrastructure as a Service (IaaS) and run government workloads in the cloud. AWS customers fully inherit the Physical Environment (PE), Media Protection (MP), and Maintenance (MA) families of controls from AWS. For the vast majority of the other security controls, customers are responsible for regulatory guidance within their AWS application, as well as documenting these implementations within their authorization package for review and approval by their authorizing official. For AWS Partner Network (APN) providers, customers can expect a range of 20-40 percent (or higher) control inheritance for the specific cloud offering. There will be controls specifically inherited from AWS (like physical/media protection), but many of the controls are shared inheritance with AWS, the CSP (PaaS/SaaS, as defined by NIST) and the end customer responsibility. Under NDA, AWS will provide an AWS FedRAMP SSP template based upon NIST 800-53v4, which is prepopulated with the applicable FedRAMP and DoD control baseline. The inherited controls within the template are prepopulated by AWS; shared controls are the responsibility of both AWS and the customer; and finally, some controls are fully the responsibility of the customer.

6.6.3. Security Practices (RFP 8.6.3)

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.*

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 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. 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.
- ▶ **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 and Practices (RFP 8.6.4)

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.

InfoReliance and AWS will not have access to any customer data. AWS provides a variety of tools and features to keep the AWS Account and resources safe from unauthorized use. This includes credentials for access control, HTTPS endpoints for encrypted data transmission, the creation of separate IAM user accounts, user activity logging for security monitoring, and Trusted Advisor security checks. You can take advantage of all of these security tools no matter which AWS services you select.

To ensure that only authorized users and processes access your AWS Account and resources, AWS uses several types of credentials for authentication. These include passwords, cryptographic keys, digital signatures, and certificates. Customers also have the option to require multi-factor authentication (MFA) to log into an AWS Account or IAM user accounts. The following table highlights the various AWS credentials and their uses.

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWS SDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.
Key Pairs	SSH login to EC2 instances CloudFront signed URLs	A key pair is required to connect to an EC2 instance launched from a public AMI. The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have a key pair generated automatically for you when you launch the instance or you can upload your own.
X.509 Certificates	Digitally signed SOAP requests to AWS APIs SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Security Credentials page.

The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The Amazon Corporate network relies on user IDs, passwords, and Kerberos, while the AWS Production network requires SSH public-key authentication through a bastion host. AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager. Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems. Requests for changes in access are captured in the Amazon permissions management tool audit log. 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 has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts.

6.6.5. List of Third-party Attestations, Reports, Security Credentials and Certifications (RFP 8.6.5)

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.

InfoReliance holds a Top Secret Facilities clearance and performs extensive work requiring personnel cleared at Top Secret, TS-SCI, and above (or comparable). We also have extensive experience with FISMA compliance, and FedRAMP ATOs for cloud solutions at both HHS and DOL. We manage Risk Management Frameworks for several DoD customers, execute cyber policies at DOE NNSA, and develop Risk Management Frameworks for DHS Einstein.

Per Q&A #395, InfoReliance is relying on additional attestations, reports, credentials, and certifications from the CSP. 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 and 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)

AWS is a FedRAMP Compliant Cloud Service Provider (CSP) and thus allows customers and partners to leverage AWS as an Infrastructure as a Service (IaaS) and run government workloads in the cloud. AWS customers fully inherit the Physical Environment (PE), Media Protection (MP), and Maintenance (MA) families of controls from AWS. For the vast majority of the other security controls, customers are responsible for federal guidance within their AWS application, as well as documenting these implementations within their authorization package for review and approval by their authorizing official. For AWS Partner Network (APN) providers, you can expect a range of 20-40+% control inheritance for your specific cloud offering. There will be controls specifically inherited from AWS (like physical/media protection), but many of the controls are shared inheritance with AWS, the CSP (PaaS/SaaS, as defined by NIST) and the end customer responsibility. Under NDA, AWS will provide an AWS FedRAMP SSP template based upon NIST 800-53v4, which is prepopulated with the applicable FedRAMP and DoD control baseline. The inherited controls within the template are prepopulated by AWS; shared controls are the responsibility of both AWS and the customer; and finally, some controls are fully the responsibility of the customer.

6.6.6. Logging Process (RFP 8.6.6)

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. Include a detailed response on how you plan to maintain security certifications.

AWS has provided a detailed plan to maintain security certifications in the AWS Risk and Compliance Whitepaper (**Attachment A**). InfoReliance attached this document for NASPO's review as part of our response to the CSA STAR requirements (**Section 6.13**).

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 internal review or external audit.

AWS CloudTrail: Features and benefits 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.

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

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

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

Reports Generated: This LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs. 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 and is an example of how to construct an Amazon Elastic MapReduce application. Customers can also customize reports generated by the LogAnalyzer.

Third Party Tools for Log Monitoring and Analysis: These are available on AWS Marketplace.

6.6.7. Visibility of Cloud Hosted Data and Documents and Restriction to Specific Users or Groups (RFP 8.6.7)

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

AWS can restrict and enables customers to restrict visibility of cloud hosted data to specific users with AWS Identity and Access Management (IAM). AWS 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, customers can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Permissions let customers 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, customers 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. Incident Response Notification Process (RFP 8.6.8)

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.

AWS has implemented various methods of external communication to support its customer base and the community. Both automated (e.g. Amazon Cloud Watch) and manual (e.g. human intervention by support personnel) mechanisms are in place to identify and respond to operational issues that impact the customer experience. A Service Health Dashboard is available (see **Figure 17** in **Section 6.12.7**) 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 a Participating Entity with security and compliance details about AWS.

As previously described in **Sections 6.2.1, 6.3.1, and 6.4**, both AWS Business Support and AWS Enterprise Support follow a detailed incident response process that specifies the timeline and mandates response times in accordance with incident levels. The InfoReliance Customer Service Representatives also cooperate with AWS support personnel with the NASPO Contract Manager as the central POC for InfoReliance awareness and escalation as required.

6.6.9. Security Controls Used to Isolate Hosted Servers (RFP 8.6.9)

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 the Participating Entity provision a logically isolated section of the Amazon Web Services (AWS) Cloud where the Participating Entity can launch AWS resources in a virtual network that they define. The Participating Entity has complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.

The Participating Entity can easily customize the network configuration for their Amazon Virtual Private Cloud. For example, the Participating Entity can create a public-facing subnet for their web servers that has access to the Internet, and place their backend systems such as databases or application servers in a private-facing subnet with no Internet access. The Participating Entity 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. Security Technical Reference Architectures (RFP 8.6.10)

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).

Figure 13 on the following page shows a security reference architecture that can be leveraged to support IaaS services. The Participating Entity can leverage many of the AWS services and complement it with their own application services to ensure the security of their workloads.

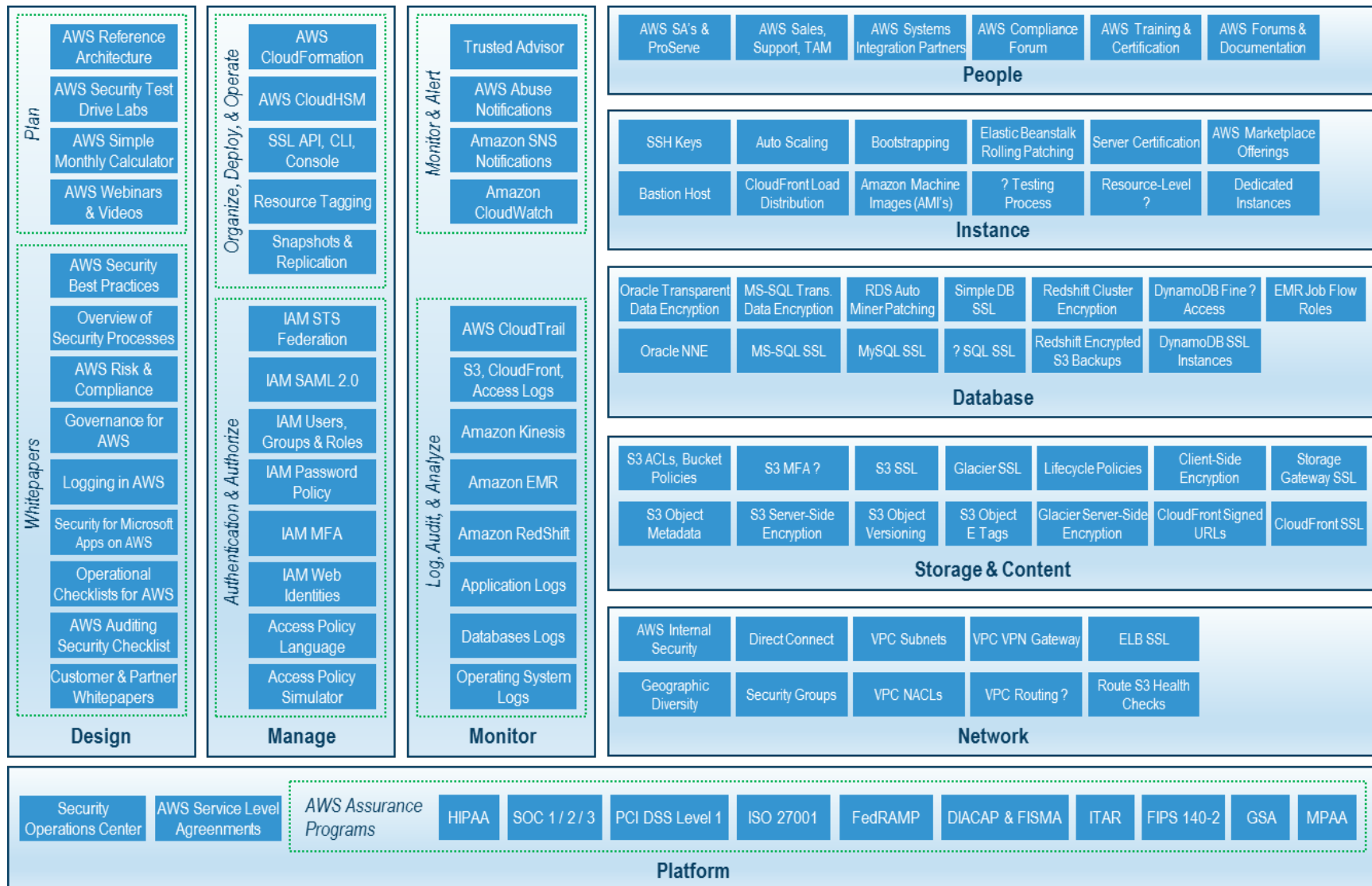


Figure 13: AWS Security Reference Architecture. The AWS Security Reference Architecture fully supports all of our IaaS offerings.

6.6.11. Security Procedures (RFP 8.6.11)

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

InfoReliance and AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security. All account access and actions are logged and restricted based on security account privileges. InfoReliance and AWS employees have no access to customer data.

6.6.12. Security Measures and Standards for Confidentiality of Data (RFP 8.6.12)

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.

InfoReliance and AWS have no access to customer data at rest or in transit. Our security measures and standards are described in detail in **Section 6.5**.

6.6.13. Policies and Procedures for Data Breach Notifications (RFP 8.6.13)

RFP 8.6.13: Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Our procedures for Data Breach notifications are described in detail in **Section 6.3.1**.

6.7. Migration and Redeployment Plan (RFP 8.7)

In this section, we demonstrate that our migration and redeployment capabilities meet or exceed the RFP requirements and should be scored **Superior**.

6.7.1. End of Life Activities (RFP 8.7.1)

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.

AWS works with customers to provide ample notice of the decommissioning of a service, or any components of a service, and continues to support customers during the transition period. For example, 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. As long as the service is active, it will meet the security, redundancy, and portability standards defined in the service offering description.

6.7.2. Return of Data (RFP 8.7.2)

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.

A Purchasing Entity has the option to pull data out of AWS by themselves, or using AWS provided native tools with portable storage devices for transport. AWS Import/Export transfers 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 upgrading connectivity. This service can be used for orderly return of data back to the Purchasing Entity.

6.8.(E) Service or Data Recovery (RFP 8.8)

In this section, we demonstrate that our approach to Service or Data Recovery meets and exceeds the RFP requirements and should be scored **Superior**.

6.8.1. Response to Situations (RFP 8.8.1)

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

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

A. Extended Downtime

AWS provides NASPO Participating Entities 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.

AWS Regions and Availability Zones can reduce, or potentially eliminate, the risks associated with extended downtime. Participating Entities can leverage these redundant virtual data centers, AZs, to spread their application components for higher availability and reduced downtime. Other services like AutoScaling and Elastic Load Balancing (ELB) can also be used to reduce extended downtime risk. With the use of AWS Regions, data can be replicated into other Regions to eliminate extended downtime. Finally, an entire application can be replicated into other Regions to eliminate the extended downtime associated with any Region or AZ. For AWS current SLA, please refer to **Section 6.10.2**. InfoReliance can work with each Participating Entity to develop high availability architectures that may eliminate the risk of extended downtime.

B. Unrecoverable Loss of Data

AWS data storage services are inherently replicated into multiple places to reduce the risk of loss of data. For example, Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance. Amazon EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component. 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.

C. System Failure

In a cloud environment, the key to risk avoidance from system failures is redundancy across cloud instances, regions, and Availability Zones. AWS minimizes any customer impact from system failures through a combination of highly available service level agreement (SLA) backed IaaS services, fully redundant design architecture options, proactive monitoring, and 24x7x365 expert support. Through the use of high availability designed architectures and a world class focus on meeting all SLAs for services, AWS IaaS services can be designed to prevent any impact to a customer from any AWS component system failure. Specifically, the use of architecture options such as multi Availability Zone, multi Region, multi instance, and real time data snapshotting allows for protection from any system downtime or data loss due to individual component failure. Additionally, AWS provides monitoring tools like CloudWatch that can be utilized to provide advance notice of any resource issues that could cause system failure. CloudWatch can be utilized to collect and track metrics, collect and monitor log files, set alarms, automatically react

to changes in AWS resources as well as custom metrics generated by applications and services, and any log files an applications generates. This provides real time system-wide visibility into resource utilization, application performance, and operational health which can be utilized to detect service issues before they experience failure. AWS also provides and 24x7x365 and industry leading technical support options for customers to support running mission critical workloads on AWS and respond to any system issue and support the highest levels of availability. In the case where AWS experiences any system failure, this multi pronged approach can prevent any customer and mission impact.

D. Recover and Restore Data within four (4) Business Hours.

AWS 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. InfoReliance works with its current customers to meets RPO/RTO requirements of multiple levels including requirements for 4 business hours. This is accomplished through a requirements driver architecture and procedures for recovering and restoring data in the event of a disaster within 4/8/24 business hours or less when needed.

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

Within AWS, it is possible to architect a solution to achieve almost any RPO and RTO required by leveraging the power of redundancy across multiple AZs and regions. AWS supports many popular DR architectures from “pilot light” environments that are ready to scale up as needed, to “warm standby” environments that enable quicker failover, and even “multi site” (active/active) environments where a service is provided by multiple regions simultaneously.

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.** Rapidly add any amount of data; easily expire/delete without handling media.
- ▶ **Security.** Secure, durable DR platform with industry-recognized certifications and audits.
- ▶ **Partners.** Solution providers and system integration partners to help with deployments.

AWS enables customers to cost-effectively operate multiple strategies as shown in **Figure 14**.

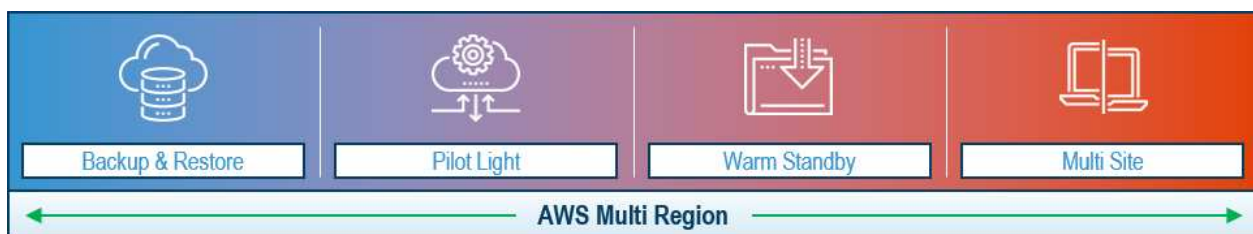


Figure 14: Spectrum of Disaster Recovery Options. AWS supports a full spectrum of DR strategies, shown here in order of how quickly the system can be available to users after a DR event.

Each DR option from **Figure 14** is discussed in detail below:

- ▶ **Backup and Restore:** A typical architecture in AWS cloud is based within a single AZ or Region. Data for this typical architecture is backed up using Amazon Simple Storage Service (Amazon S3) 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. To provide additional DR capabilities, the backed up S3 data can be replicated into a different Region. In the case of a disaster, data can be recovered from the other Region.
- ▶ **Pilot Light for Simple Recovery into AWS Warm Standby Solution:** In a gas heater, a pilot light is a small idle flame that's always on and can quickly ignite the entire furnace to heat up a house as needed. In AWS DR, a "pilot light" solution ensures that customers have the critical core elements of their system already configured and running in a different AWS Region - the pilot light. Then, when the time comes for recovery, customers simply provision a full-scale production environment around the critical core in that second Region.
- ▶ **Warm Standby Solution in AWS:** In a "warm standby" architecture, a scaled-down version of a fully functional environment is always running in a second AWS Region. This architecture further decreases recovery time because some services are always running. By identifying business-critical systems, customers could fully duplicate these systems on AWS in a second Region and have them always on.
- ▶ **Multi-Site Solution Deployed on AWS and On-Site:** A multi-site solution runs in AWS in multiple Regions in an active-active configuration. During a disaster situation of an entire Region, an organization can simply send all traffic to AWS servers in the second Region, which can scale to handle their full production load.

Amazon S3

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.

DR Resources: There are multiple resources to help organizations start using AWS for a DR/COOP and backup solution. We encourage Participating Entities to read and review the following resources as they make best value determinations:

- ▶ 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](#)

6.8.2. Methodologies for Backup and Restore Services (RFP 8.8.2)

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.

A. Data Backups The AWS platform enables a lightweight approach to backup and recovery, which includes 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 web server instance, 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 such as 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. **Figure 16** depicts an Amazon EC2 approach.

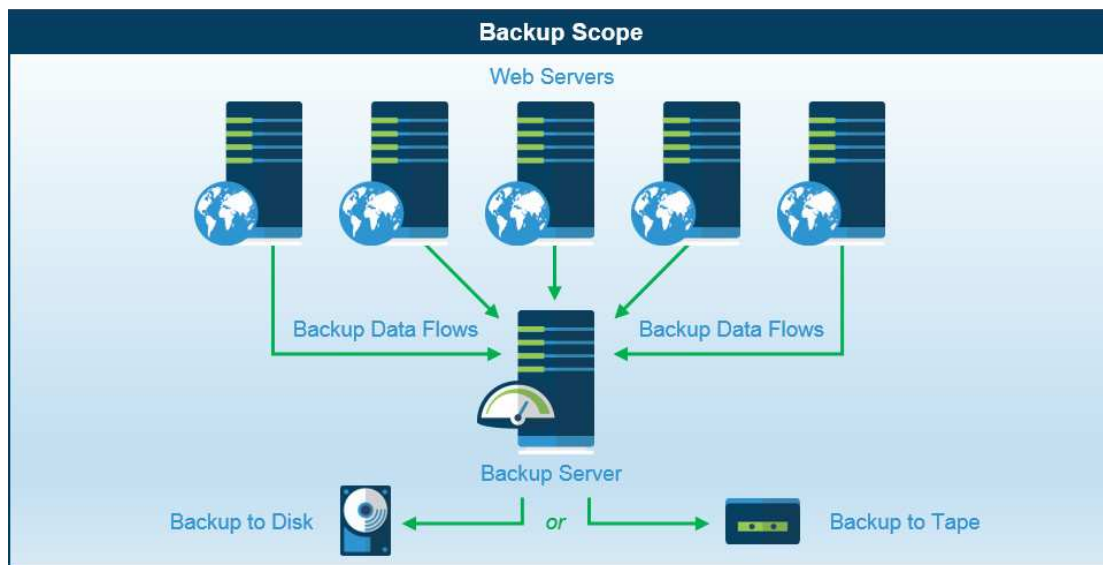


Figure 15: Traditional Backup Approach. *This approach requires substantial infrastructure overhead and saving all information from all servers to disk and/or tape.*

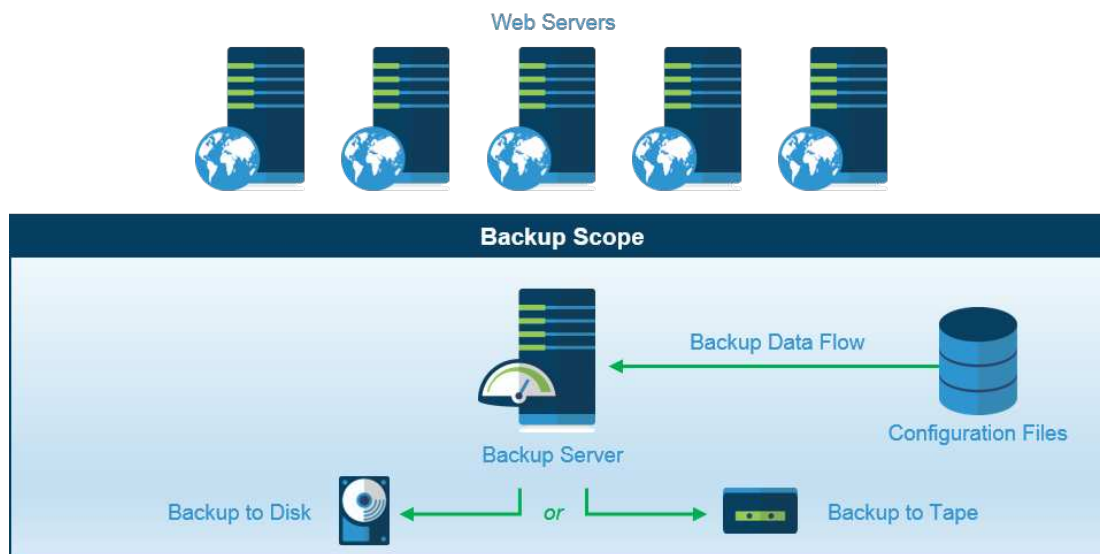


Figure 16: Amazon EC2 Backup Approach. *This superior approach requires substantially less infrastructure and offers faster recovery time because only configuration files and images are saved.*

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). The only components requiring backup and recovery are the AMI and configuration file(s).

Configuration Files: Customers use a variety of version management approaches for configuration files, and they can follow the same regimen 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.

B. Method of Server Image Backups 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. 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. Customers can also create multiple copies of the AMI within the same account.

C. Digital Location of Backup Storage

AWS provides multiple storage options that leverage multiple Regions and Availability Zones where backup data is stored. For example, Amazon Simple Storage Service (Amazon S3) is storage for the Internet. A Purchasing Entity can use Amazon S3 to store and retrieve any amount of data, at any time, from anywhere on the web. They can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console. S3 data is replicated multiple times in a Region. For additional storage, data can also be automatically replicated in other Regions. Similarly, Amazon Glacier is a storage service optimized for infrequently used data, or "cold data." The service provides secure, durable, and extremely low-cost storage for data archiving and backup. With Amazon Glacier, a Purchasing Entity can store their data cost effectively for months, years, or even decades. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so they do not have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations. Glacier data has the same replication approach as S3.

D. Alternate Data Center Strategies (Continental United States) 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 a Purchasing Entity 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 with four (4) new regions coming soon.

In the Continental United States, AWS has four (4) existing regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), and AWS GovCloud (US) (Oregon). An additional region will soon be added in Ohio.

6.9.(E) Data Protection (RFP 8.9)

In this section, we demonstrate that technical capabilities and policies for Data Protection meet and exceed the RFP requirements and should be scored **Superior**.

6.9.1. Standard Encryption Technologies / Protecting Sensitive Data (RFP 8.9.1)

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.*

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. Available tools include Loop- AES, dm-crypt (with or without) LUKS, and TrueCrypt. Each of these operates below the file system layer using kernel space device drivers to perform encryption and decryption of data. Another option would be to use file system-level encryption, which works by stacking an encrypted file system on top of an existing file system. This method is typically used to encrypt a specific directory. eCryptfs and EncFS are two Linux-based open source examples of file system-level encryption tools. These solutions all require a

Participating Entity to provide keys, either manually or from their KMI. Encrypting Amazon EBS volumes attached to Windows instances can be done using BitLocker or Encrypted File System (EFS) as well as open source applications like TrueCrypt. In either case, you still need to provide keys to these encryption methods and you can only encrypt data volumes.

For object storage, Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. A Participating Entity has the following options of protecting data at rest in Amazon S3.

- ▶ Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- ▶ Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Additional information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (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 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.

6.9.2. Business Associate Agreements (RFP 8.9.2)

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.

InfoReliance is willing to sign relevant and applicable Business Associate Agreements and any other necessary agreements with Participating Entities to protect data.

6.9.3. How InfoReliance Will Use Data (RFP 8.9.3)

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.

InfoReliance and AWS will only use data for purposes defined in the Master Agreement. Neither InfoReliance nor AWS will use the government data or government related data for any other purpose including but not limited to data mining nor resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

6.10. (E) Service Level Agreements (RFP 8.10)

AWS offers industry leading Service Level Agreements to support high availability and scalable solutions for mission critical workloads. In this section, we demonstrate that our Service Level Agreements meet and exceed the RFP requirements and should be scored **Superior**.

6.10.1. Negotiable Service Level Agreement (RFP 8.10.1)

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.

AWS SLAs are specific to each individual IaaS offering and are not negotiable. Accepting AWS commercially published SLAs benefits the Purchasing Entity because standardization keeps CSP costs low. InfoReliance Service Level Agreements as applicable are negotiable based on specific customer requirements for each engagement.

6.10.2. Sample of Service Level Agreement (RFP 8.10.2)

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.

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 the AWS website. For the convenience of reviewers, we have downloaded the following set of SLAs (current as of the time of submission) and provided them as **Attachment B – AWS Sample SLAs**. We have also provided the URLs as a courtesy.

AWS Service	SLA Commitment	Courtesy URL
EC2	Monthly Uptime % of at least 99.95%	http://aws.amazon.com/ec2-sla/
S3	Monthly Uptime % of at least 99.9%	http://aws.amazon.com/s3-sla
CloudFront	Monthly Uptime Percentage of at least 99.9%	http://aws.amazon.com/cloudfront/sla/
Route 53	100% Available	http://aws.amazon.com/route53/sla/
RDS	Monthly Uptime Percentage of at least 99.95%	http://aws.amazon.com/rds-sla/

6.11. (E) Data Disposal (RFP 8.11)

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

In this section, we demonstrate that our data disposal procedures, policies, and confirmation process meet and exceed the RFP requirements and should be scored **Superior**.

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. Additional key aspects regarding data ownership and management in the cloud are based on shared responsibility model, and include the following:

- ▶ InfoReliance and AWS have no access to customer data.
- ▶ The Physical Environments continue to own their data.
- ▶ The Physical Environments choose the geographic location(s) in which to store their data—it does not move unless the Participating Entity decides to move it.
- ▶ The Participating Entity can download or delete their data whenever they like. The Physical Environment 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 the Physical Environments with the ability to delete their data. However, AWS customers retain control and ownership of their data, and it is the Physical Environment's responsibility to manage their data lifecycle

6.12. (E) Performance Measures and Reporting (RFP 8.12)

In this section, we demonstrate that our Performance Measures and Reporting meet and exceed the RFP requirements and should be scored **Superior**.

6.12.1. Guaranteed Reliability and Uptime (RFP 8.12.1)

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.

AWS services such as EC2 and RDS guarantee availability greater than 99.9%. Based on specific customer requirements, InfoReliance can design and architect all AWS services to guarantee availability greater than 99.9%.

6.12.2. Standard Uptime and SLA Criteria (RFP 8.12.2)

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

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 the AWS website. For the convenience of reviewers, we have downloaded the following set of SLAs (current as of the time of submission) and provided them as **Attachment B – AWS Sample SLAs**. We have also provided the URLs as a courtesy.

AWS Service	SLA Commitment	Courtesy URL
EC2	Monthly Uptime % of at least 99.95%	http://aws.amazon.com/ec2-sla/
S3	Monthly Uptime % of at least 99.9%	http://aws.amazon.com/s3-sla
CloudFront	Monthly Uptime Percentage of at least 99.9%	http://aws.amazon.com/cloudfront/sla/
Route 53	100% Available	http://aws.amazon.com/route53/sla/
RDS	Monthly Uptime Percentage of at least 99.95%	http://aws.amazon.com/rds-sla/

6.12.3. Support Contact (RFP 8.12.3)

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.

InfoReliance will provide standard Customer Support for value-added services. AWS Business Support is required under the AWS Reseller program, with an additional Enterprise Support option. **Sections 6.2.1, 6.3.1, and 6.4** describe the contact process, incident response process, and exceptional levels of CSR responsiveness. The table in **Section 6.3.1B** compares and contrasts the Business and Enterprise Support options. Both offer direct access to AWS Cloud Support Engineers with 24x7x365 availability by email, chat, or phone.

6.12.4. Consequences/SLA Remedies for Incidents (RFP 8.12.4)

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

AWS offers the following SLA remedies as outlined in the table below. To make a claim, Customers simply email the claim with supporting logs within 30-60 days for credit on the next invoice from InfoReliance for AWS IaaS services.

Service	SLA Commitment	Specifics	Definitions
S3	Monthly Uptime % of at least 99.9%	▪ Equal to or greater than 99% but less than 99.9% = 10% credit	▪ Error rates = errors/requests every 5 minutes
		▪ Less than 99% = 25% credit	▪ Uptime = 100%- % avg error rate avg for 5 minute periods
RDS	Monthly Uptime Percentage of at least 99.95%	▪ Less than 99.95% but equal to or greater than 99.0% = 10% credit	▪ Uptime = 100% - % of 1 minute periods not available
		▪ Less than 99.0% = 25% credit	
CloudFront	Monthly Uptime Percentage of at least 99.9%	▪ Equal to or greater than 99% but less than 99.9% = 10% credit	▪ Error rates = errors/requests every 5 minutes
		▪ Less than 99% = 25% credit	▪ Uptime = 100%- % avg error rate avg for 5 minute periods
EC2/EBS	Monthly Uptime % of at least 99.95%	▪ Less than 99.95% but equal to or greater than 99.0% = 10% credit	▪ Uptime = 100% - % minutes not available
		▪ Less than 99.0% = 30% credit	
Route 53	100% Available	▪ 5 - 30 minutes + 1 day credit	▪ Available = did not fail to respond to DNS queries
		▪ 31 minutes - 4 hours = 7 day credit	
		▪ More than 4 hours = 30 day credit	
AWS Support Desk	Phone, Chat, Email (24/7)	▪ No credit	
	Support Level Enterprise: Case Severity & Response Times*		
	Critical: < 15 minutes		
	Urgent: < 1 hour		
	High: < 4 hours		
	Normal: < 12 hours		
	Low: < 24 hours		

6.12.5. Downtime Procedures and Schedules (RFP 8.12.5)

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

AWS services are highly available (up to 99.9999%) and therefore we do not schedule or plan for downtime. For value-added services, InfoReliance will employ its rigorous iFRAME quality management system (see **Section 6.4.1A**). The project management discipline includes detailed guidelines for schedule management and coordination with customers. InfoReliance will avoid planned downtime if at all possible and when unavoidable, will provide timely advance notice to the customer for acceptance and approval without disrupting the customer's mission.

6.12.6. Consequences/SLA Remedies for Disaster Recovery (RFP 8.12.6)

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

Please see the SLA Remedies table in **Section 6.12.4** above and specifically the Uptime metrics.

6.12.7. Sample of Performance Reports (RFP 8.12.7)

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 provides all customers real time, up-to-the-minute statistics for performance reporting through the AWS Service Health Dashboard. The dashboard is available 24x7. Customers can visit the URL (<http://status.aws.amazon.com/>) at any time for current status information or subscribe to an RSS feed with notifications for each individual service. **Figure 17** below shows a recent screenshot of the current status portion of the dashboard:

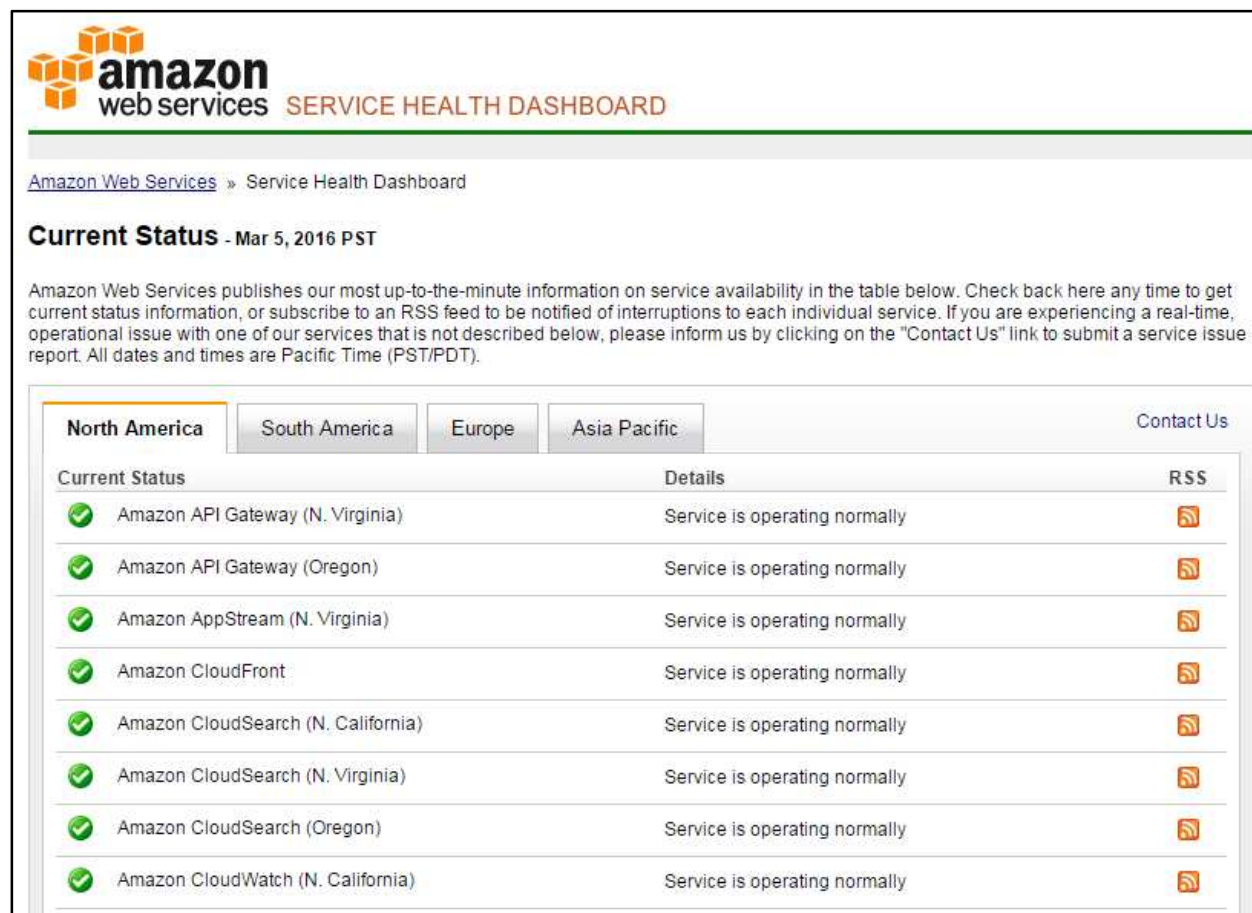


Figure 17: Sample Performance Report (Real Time). The AWS Service Health Dashboard is available to customers 24x7 and provides real time, up-to-the-minute status and performance information.

AWS also maintains a running log of service interruptions as part of the Service Health Dashboard. This data is also available 24x7 in real time and extends back 12 months. **Figure 18** is a recent screenshot of the dashboard showing Status History:

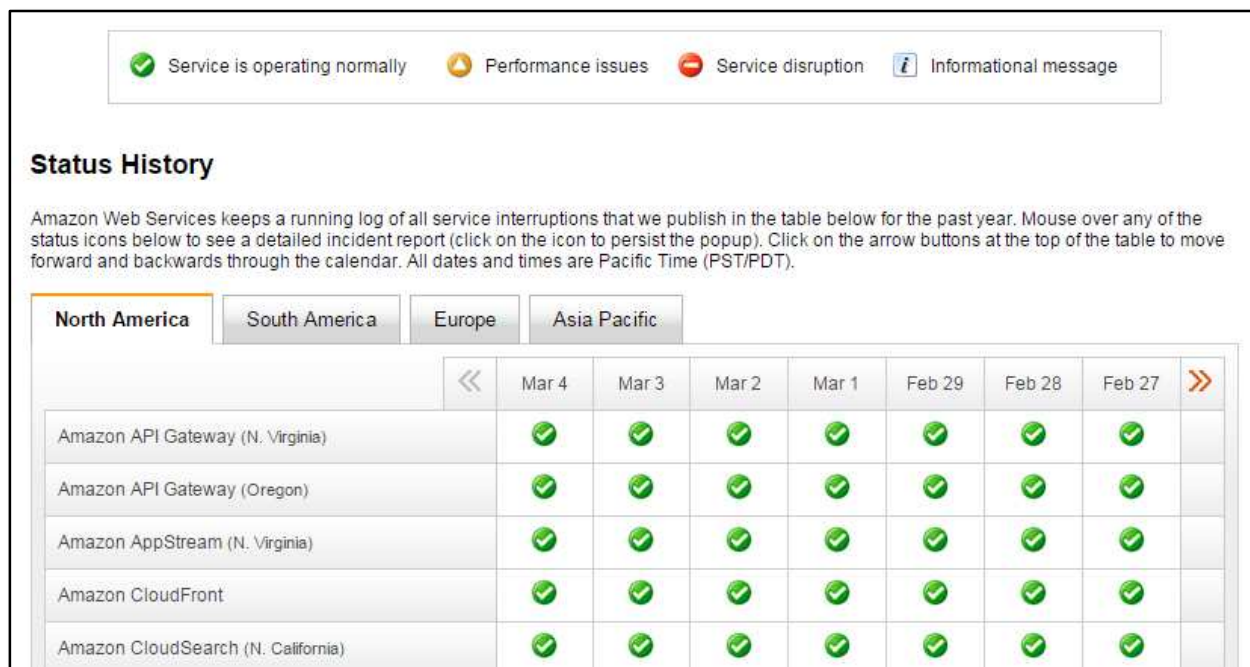


Figure 18: Sample Performance Report (Historical). The AWS Service Health Dashboard includes details of any service interruptions for the last 12 months.

To view a detailed incident report, click one of the status icons for a report to popup.

To move forwards and backwards through the calendar, click on the double orange arrows located at the top of the table.

6.12.8. Ability to Print Reports Locally (8.12.8)

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

AWS historical and statistical reports may be printed locally from the AWS Service Health Dashboard as shown above. Usage reports are available via both local printer options and also through the iRAMP console.

6.12.9. On-demand Deployment Support (RFP 8.12.9)

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

AWS supports on-demand deployment of AWS services 24x7x365. The NIST on-demand self service capability is met by AWS through the AWS Management Console—a web application for managing Amazon Web Services.

The console provides an intuitive user interface for performing many AWS tasks. This includes working with Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting Amazon CloudWatch alarms, and more. Customers can access each service from the AWS Management Console, which also provides information about accounts and billing.

To perform on-demand deployment, start by clicking **Services** located at the top of the page. A full dropdown list of available AWS services will appear, as shown in **Figure 19**.

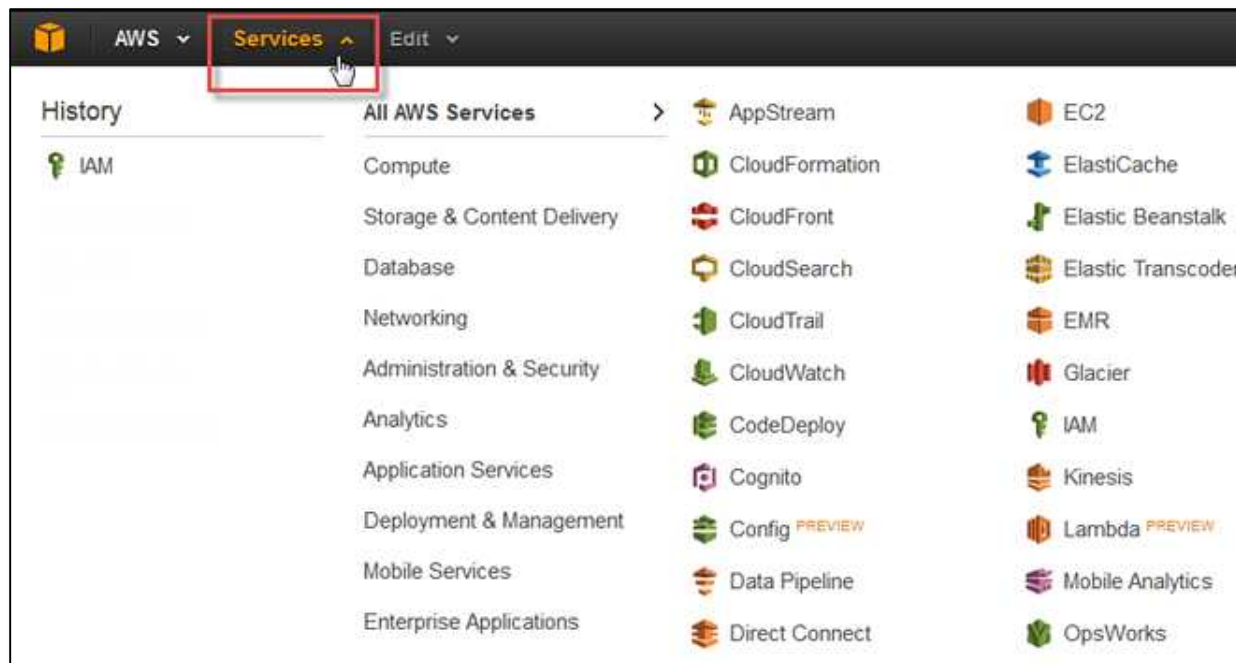


Figure 19: Accessing the Full List of Services.

To search for a list of available services within a specific category, such as **Compute & Networking**, hover over the category and click a service name to open the console for that service and use the AWS NIST compliant on-demand self-service (**Figure 20**).



Figure 20: How to Access a List of Available Services in a Category.

6.12.10. Scale-up and Scale-down Availability (RFP 8.12.10)

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

AWS offers scale up/down 24x7x365. Customers can scale up/down new instances of virtual machines with a few clicks. For the *automated* scale up/down, customers can use AWS Auto Scaling service. AWS Auto Scaling helps customers maintain application availability and allows them to scale their Amazon EC2 capacity up or down automatically according to conditions they define. Customers can use Auto Scaling to help ensure that they are running their desired number of Amazon EC2 instances. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls.

to reduce costs. Auto Scaling is well suited both to applications that have stable demand patterns or that experience hourly, daily, or weekly variability in usage.

6.13. (E) 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.
- b. Completion of Exhibits 1 **and** 2 to Attachment B.
- c. Completion of a CSA STAR Attestation, Certification, or Assessment.
- d. Completion CSA STAR Continuous Monitoring.

In this section, we demonstrate that our CSA credentials meet and exceed the RFP requirements and should be scored **Superior**.

Per Q&A #85, if the CSP (AWS) satisfies this requirement as the manufacturer, the requirement is also satisfied for the reseller (InfoReliance). InfoReliance is submitting all of the following materials on behalf of AWS and for all proposed AWS offerings.

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. AWS continues to raise the bar on CSA's "attestation" and "certification" program.

A. Level 1 CSA STAR Registry Self-Assessment

This is contained within pp 25-61 of **Attachment A – AWS Risk and Compliance Whitepaper**.

B. Exhibits 1 and 2 to RFP Attachment B

AWS asserts that **Attachment A – AWS Risk and Compliance Whitepaper** satisfies both of these Exhibits. The completed Consensus Assessments Initiative Questionnaire (CAIQ) is the latest version (v3) released by CSA and includes mappings to the standards and controls in the Cloud Controls Matrix (CCM).

C. Level 2 CSA STAR Registry Assessment Certification

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

- ▶ **SOC 2:** This audit report attests that AWS has been validated by a third party auditor to confirm that the AWS control objectives are appropriately designed and operating effectively. We cannot provide the SOC 2 audit report in a proposal but it can be requested under NDA (<http://aws.amazon.com/compliance/contact>).
- ▶ **ISO 27001:2005:** We have provided this AWS certification as **Attachment D – AWS ISO 27001 Certification**.

D. 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 our approach to conducting continuous monitoring within the FedRAMP Security Assessment Framework. AWS only provides this plan to customers as part of its AWS FedRAMP package, which may be requested under a Nondisclosure Agreement at <https://aws.amazon.com/compliance/contact>. This plan 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.

6.14. (E) Service Provisioning (8.14)

In this section, we demonstrate that our service provisioning capabilities meet or exceed the RFP requirements and should be scored **Superior**. AWS offers 100% self service and on-demand provisioning through the AWS Management Console and also current pricing for all services through the AWS online calculator for customers who have awarded in scope contracts and

funding in place. As an additional option, customers can utilize the InfoReliance customer service representative support for assistance with new service quotes, account setup and provisioning.

6.14.1. Emergency or Rush Services Implementation Requests (RFP 8.14.1)

RFP 8.14.1: Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

InfoReliance exceeds this requirement with 24x7x365 on-demand deployment of AWS services. As services are needed, customers have full control to deploy with no lead time. For additional details on how on-demand provisioning works to meet any required customer timeline, see **Section 6.12.9**

6.14.2. Standard Lead-time for Provisioning Solutions (RFP 8.14.2)

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

InfoReliance also exceeds this requirement. There is no standard lead time for provisioning AWS services. They are available 24x7x365 and on-demand with full customer control. For additional details on how on-demand provisioning works, see **Section 6.12.9**

6.15. (E) Backup and Disaster Plan (RFP 8.15)

In this section, we demonstrate that our back up and disaster planning capabilities meet or exceed the RFP requirements and should be scored **Superior**.

6.15.1. Apply Retention Periods and Disposition (RFP 8.15.1)

RFP 8.15.1: Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

S3 and Glacier storage services used by backup and disaster plans allow Participating Entities to establish a retention period using lifecycle policies associated with these services. Participating Entities will be able to apply legal retention periods and disposition by agency in accordance with their policies and/or legal requirements.

6.15.2. Disaster Recovery Risks and Mitigation (RFP 8.15.2)

RFP 8.15.2: Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

With AWS, Participating Entities 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 Participating Entities 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 capabilities to minimize the inherent risks of traditional DR:

- ▶ **Fast Performance:** Fast, disk-based storage and retrieval of files as opposed to inherent risk of slow retrieval.
- ▶ **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:** Quickly add any amount of data; easily expire/delete without handling media.
- ▶ **Security:** Secure, durable DR platform with industry-recognized certifications and audits.
- ▶ **Partners:** Solution providers and system integration partners to help with deployments.

6.15.3. Infrastructure that Supports Multiple Data Centers (RFP 8.15.3)

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.

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 Participating Entities 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 uninterruptible 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.

Participating Entities 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 scenarios, including natural disasters or system failures. However, Participating Entities should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between regions unless proactively done so by the Participating Entity, thus allowing Participating Entities 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 four regions in the United States: **1.** US East (Northern Virginia) **2.** US West (Oregon), **3.** US West (Northern California), and **4.** AWS GovCloud (US).

6.16. (E) Solution Administration (8.16)

In this section, we demonstrate that our Solution Administration capabilities meet or exceed the RFP requirements and should be scored **Superior**.

6.16.1. Management of Identity and User Accounts (RFP 8.16.1)

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

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

6.16.2. Anti-Virus Protection (RFP 8.16.2)

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

End-to-end secure computing environment, AWS employs a shared security responsibility model with its customers. While AWS provides secure facilities and processes, it is up to its customers to protect their operating systems, applications and data running on AWS. It is important to understand the division of shared responsibilities between AWS and the Participating Entities. AWS provides the ability to provide anti-virus protection for data stores like EBS volumes using multiple anti-virus solutions, including through the AWS marketplace.

6.16.3. Migrating Data (RFP 8.16.3)

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

AWS Import/Export provides the ability to migrate large amounts of data into and out of AWS using physical storage appliances, bypassing the Internet in three ways:

- 1) AWS Import/Export transfers data directly onto and off of appliances using the Amazon high-speed internal network, bypassing the Internet entirely.
- 2) AWS Import/Export Disk is used for normal data loads.
- 3) AWS Import/Export Snowball (Snowball) is used for large data loads.

6.16.4. Ability to Administer Solution (RFP 8.16.4)

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

Participating Entities can administer the solution independently of one another and in a distributed manner within their own organizations through access to AWS Management using group and roles within Identity and Access Management dashboard. Each group has a defined set of access controls and responsibilities. This ability to administer solution across multiple entities within and organization can be taken a step further by building each solution in a separate VPC, and provide VPC peering between these VPCs with appropriate access control and permissions. A VPC peering connection is a networking connection between two VPCs that enables routing traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. Organizations can create a VPC peering connection between their own VPCs, or with a VPC in another AWS account within a single region.

6.16.5. Ability to Apply Defined Administration Policies (RFP 8.16.5)

RFP 8.16.5: Ability to apply a participating entity's defined administration policies in managing a solution.

Participating Entities can grant permissions to IAM entities (users, groups, and roles). By default, these entities start with no permissions and can do nothing in AWS until granted permissions. To give entities permissions, the Participating Entity can attach a policy that specifies the type of access, the actions that can be performed, and the resources on which the actions can be performed. In addition, the Participating Entity can specify any conditions that must be set for access to be allowed or denied.

To assign permissions to a user, group, role, or resource, the Participating Entities can create a policy, which is a document that explicitly lists permissions. In its most basic sense, a policy lets the Participating Entity specify the following:

- ▶ **Actions:** what actions the Participating Entity will allow. Each AWS service has its own set of actions. For example, the Participating Entity might allow a user to use the Amazon S3 ListBucket action, which returns information about the items in a bucket. Any actions that the Participating Entities do not explicitly allow are denied.
- ▶ **Resources:** which resources the Participating Entity allows the action on. For example, permissions determine on which Amazon S3 buckets the user may perform the ListBucket action. Users cannot access any resources unless first explicitly granted permissions.
- ▶ **Impact:** what the effect will be when the user requests access—either allow or deny. The default state is that resources are denied to users unless explicitly granted permissions.

6.17. (E) Hosting and Provisioning (RFP 8.17)

In this section, we demonstrate that our hosting and provisioning processes, capabilities, and especially our toolsets meet or exceed the RFP requirements and should be scored **Superior**.

6.17.1. Cloud Hosting and Provisioning Process (RFP 8.17.1)

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

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. They 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.

6.17.2. Minimum Toolsets (RFP 8.17.2)

RFP 8.17.2: Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)
2. Creating and storing server images for future multiple deployments
3. Securing additional storage space
4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Tool Sets for Deploying New Servers: NASPO Participating Entities will be able to deploy all purchased services on-demand 24x365 through the AWS Management Console. 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. Purchasing Entities can use the AWS Management Console to perform any number of tasks, from deploying servers to monitoring the health of applications. The AWS Management Console also enables NASPO 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 NASPO customers provision resources across multiple regions. Customers may also utilize the AWS Command Line Interface (CLI) is a unified tool to manage AWS services. The CLI services requires one tool to download and configure that can control multiple AWS

services from the command line and automate them through scripts. Additionally, AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS API-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits. Customers can use AWS Software Development Kits (SDK) to programmatically provision or manage IaaS without any interaction with IR or AWS.

Tool Sets for Creating and Storing Server Images: Toolsets for creating and storing images are available in the AWS EC2 dashboard or through AWS API. 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. Customers can create and store copies of the AMI by starting a new instance based upon the shared AMI and then creating a new AMI from that instance. Customers can also create multiple copies of the AMI within the same account.

Tool Sets for Securing Additional Storage Space: Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are network-attached, and persist independently from the life of an instance. Additional storage space can be secured through the AWS Management Console or through well-defined and documented Application Programming Interfaces (APIs).

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

6.18. (E) Trial and Testing Periods (Pre-And Post-Purchase) (RFP 8.18)

In this section, we demonstrate that our trial and testing periods meet or exceed the RFP requirements and should be scored **Superior**.

6.18.1. Testing and Training Periods (RFP 8.18.1)

RFP 8.18.1: Describe your testing and training periods that your offer for your service offerings.

InfoReliance and AWS work with their customers to provide testing and training periods of their service offerings. These include webinars, quick start guides, and other forms of training ranging from introductory to advanced. AWS offers self-paced labs for training and testing. InfoReliance has created a suite of AWS Test Drives for customers to experiment with specific applications such as SharePoint, McAfee, or ESRI ArcGIS.

6.18.2. Test and/or Proof of Concept Environment for Evaluation (RFP 8.18.2)

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.

If a Participating Entity needs to evaluate an AWS service against a set of requirements, InfoReliance will work with the customer to establish a test or proof of concept environment for their workloads. InfoReliance is currently managing a proof of concept environment for the entire Department of Health and Human Services (HHS) as a cloud sandbox for individual HHS agencies to evaluate AWS IaaS offerings.

6.18.3. Training and Support at No Additional Cost (RFP 8.18.3)

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

AWS offers extensive training and support for their service offerings at no additional cost. This training and support is continually refreshed and updated to reflect the latest AWS services, with hundreds of new features and updates each year. This training and support is freely available online and includes the following:

- ▶ Online AWS training videos to help customers ramp up on AWS services
- ▶ Online AWS labs that provide hands-on practice with live AWS services
- ▶ Online Knowledge Center
- ▶ AWS Support Center and Support FAQs
- ▶ AWS Support Documentation (features, specifications, and instructions)
- ▶ AWS White Papers

6.19. (E) Integration and Customization (RFP 8.19)

In this section, we demonstrate that our integration and customization capabilities meet or exceed the RFP requirements and should be scored **Superior**.

6.19.1. Solutions Integrated to Complementary Applications (RFP 8.19.1)

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 services are based on a RESTful API that can be leveraged to integrate with other complementary applications. AWS API is a standard interface that partners, software vendors, and customers like a Participating Entity can use to integrate their existing applications with AWS. Additionally, InfoReliance has extensive expertise in both custom of the shelf (COTS) and customer application development and as part of the optional value added services can provide integration and customization capabilities. As an example, InfoReliance is currently providing fully managed Microsoft SharePoint platforms deployed in AWS and integrated with other third party platforms like Brightworks as a fully managed MSP solution for amazon.com. This capability is a key differentiator for InfoReliance for our customers.

6.19.2. Customize and Personalize the Solutions (RFP 8.19.2)

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

To customize and personalize the solutions, AWS offers Amazon API Gateway as a fully managed service for developers to easily create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, a Participating Entity can create an API that acts as a “front door” for applications to access data, business logic, or functionality from its back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any Web application. Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. InfoReliance has successfully utilized Amazon API for customers to customize and personalize AWS deployed solutions to include a fully customized content sharing website for the General Accounting Office (GAO) that allows for information collaboration to meet GAO specific requirements and deployed in the cloud.

6.20. (E) Marketing Plan (RFP 8.20)

RFP 8.20: Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

In this section, we demonstrate that our Marketing Plan meets and exceeds the RFP requirements and should be scored **Superior**.

InfoReliance will leverage extensive, award-winning demand generation and marketing expertise to encourage Participating Entities to adopt the NASPO contract and establish Participating Addendums for our cloud solutions. We have been highly successful marketing these solutions

and services to Federal customers through our portfolio of Government Wide Acquisition Contracts (GWACS) and will adapt a similar approach to demonstrating the benefits of cloud services to the Participating Entities. Our Marketing Plan includes the following:

- ▶ Dedicated NASPO Cloud Solutions page on the InfoReliance website, with a complete listing of available services, ordering instructions for Participating Entities, FAQs, contact information, and a link to the self-service AWS calculator. This will be developed within 30 days of the Master Agreement award.
- ▶ Digital media programs to reach potential customers and build awareness of our cloud service offerings under the NASPO agreement
- ▶ InfoReliance white papers and other publications demonstrating thought leadership
- ▶ Social media including LinkedIn, Twitter, and other channels
- ▶ AWS publications such as the white paper *The Total Cost of (Non) Ownership of Web Applications in the Cloud*
- ▶ AWS tools such as the Total Cost of Ownership (TCO) Calculator
- ▶ Speaking at conferences and other industry events such as the AWS Public Sector Symposium, AWS Reinvent Conference, ESRI Federal Conference, McAfee User Conference, RSA Archer User Conference as examples.
- ▶ Partner briefings to strategic partners such as Microsoft, ESRI, AWS, McAfee
- ▶ Direct sales with a national business development team covering the US public sector

6.21. (E) 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.

In this section, we demonstrate that InfoReliance meets and exceeds the requirements for related value-added services as described in **RFP 8.21** and should be scored **Superior**.

6.21.1. Professional Services for Initial Setup, Training, and Access to Services

A strategic value added benefit that InfoReliance offers to the NASPO community is an extensive level of cloud technical and functional consulting expertise. As an AWS Advanced consulting partner and Audited AWS Managed Service Provider (MSP), InfoReliance is currently providing value added services to more than 30 public sector cloud customers. We have a proven track record of deploying both required and optional IaaS workloads into AWS utilizing an agile software development lifecycle framework, quality systems based on CMMI, ISO, and ITIL, and lean startup methodologies to successfully deliver e-government-wide solutions and shared services for all stakeholders. Our customers often start with cloud IaaS resale and then quickly reach out to us for additional support around consulting and managed services along their cloud adoption lifecycle. These core IaaS value added services include initial setup provisioning and access to the services so that customer can effectively use IaaS NIST and FedRAMP compliant services starting Day One. Customers can then provision additional services on a true on-demand model going forward, with no lead time whatsoever. In addition, throughout our 15 year history, InfoReliance has focused on application solution development to meet our customer's mission. Because we can offer IaaS platforms and complete cloud migration services, our customers benefit from having a one stop partner to meet all their IaaS, consulting, and MSP needs.

InfoReliance delivers these solutions through more than 250 certified AWS Cloud Solutions Architects and accredited professionals who receive constant training and education through the InfoReliance Cloud University (ICU) on the latest cloud services. ICU has proven so successful that we offer these same services and training to our Customers in standard and custom offerings to include FBI, HHS, TVA, and many others. We have trained more than 700 students so far and continue to focus on this core cloud value added service.

InfoReliance offers the following Value Added Services related to initial setup, provisioning, access to the services, and training.

Required Service	InfoReliance Description Overview
Virtual Private Cloud Setup	Create the VPC, subnets, and network ACLS.
EC2 Provisioning	Launch the EC2 instance and EBS volumes.
Billing and Invoice Setup	Set up the appropriate billing codes and invoicing for the customer.
Billing and Invoice Management	Provide monthly invoices and manage billing activities.
Project Management	Oversee project activities.
AWS Account Provisioning	Create the AWS Account and IAM users and roles to manage the AWS resources.
AWS Services Configuration	Perform basic account configurations such as password policies, CloudTrail logging, and IAM roles.
Identity and Access Management and Single Sign on	Create granular permissions for IAM Users, Groups, and Roles. Ensure Roles are used throughout the infrastructure.
Project Deliverables	Provide required contract deliverable items to the customer at specified deadlines.
Quality Assurance Metrics and Reporting	Record, analyze, and provide basic metric reports for basic QA purposes.
Project Status Reports	Provide required basic monthly/weekly project status reports.
AWS 24x7x365 Support	Configure AWS Business Support account with 24x7x365 support from designated AWS customer representatives.
Help Desk Portal	Create a customer service workspace and email contact for the customer and customer service support.
Training	Based on customer requirements InfoReliance offers both standard and customer IaaS training courses through ICU. Start offerings include Cloud Essentials, Architecture, Advanced Architecture, Systems Operations, Application Development, DevOps, Big Data, Security, Migration. Custom training is also available based on specific customer requirements to meet their mission and objectives.

6.21.2. Related Services for Optional Use by Participating Entities

The Q&A (#517 and #530) as well as the Cost Proposal instructions list a wide range of additional services that may be desired by Purchasing Entities. We have provided fully burdened hourly rates in the Cost Proposal for any optional services added to a Participating Addendum.

InfoReliance customers often request additional services including but not limited to the following:

- ▶ Infrastructure as a Service (IaaS)
- ▶ High developer involvement
- ▶ Application modifications to optimize or deploy cloud solutions
- ▶ Database/application administration
- ▶ Systems engineering and configuration services
- ▶ Cloud consulting services (e.g. an agency Cloud Roadmap)
- ▶ Cloud Single Sign-on
- ▶ Disaster Recovery
- ▶ Big Data and analytics
- ▶ Cloud migration
- ▶ Office 365 mailbox migration with email, collaboration, and instant messaging

The table below provides an overview of additional available cloud services:

Optional Service	InfoReliance Description Overview
Operating system hardening at deployment	The deployed operating system will receive the current approved customer security baseline as required.
STIG compliance updates	Within 14 days of a new STIG configuration being approved, instances will be updated with the new STIG settings.
Operating system patching	At the time of deployment, the instance will have all applicable Operating System patches. Within 14 days of a patch being released, it will be applied to the baseline AMI and existing, non-production instances. Production systems will be redeployed from the baseline.
Monthly vulnerability scans	Within the first 5 business days of each month, a vulnerability scan assessing the SCAP compliance and Operating System patch level will be performed on each instance using a credentialed scan. The scans will be placed in S3 and provided to the customer.
Log retention and archiving (CloudWatch)	AWS API call logging and retention.
VPC and IP management	Maintain IP Address Management (IPAM) for the VPC and allocate appropriate IP space.
Storage management	Monitor S3, EBS, and Glacier utilization. Create buckets and provision EBS volumes.
Database Management	Perform capacity and performance management on provisioned RDS instances.
Basic Disaster recovery / backup management	Take basic EBS snapshots for data recovery and backups.
Enhanced Backup	Provide the capability to quickly recover from a service interruption with minimal loss of data and ensure the integrity of the data and remove single points of failure. The backup solution and processes will focus on Servers, Database, and Static Content.
Cloud Data Archival	Provides several capabilities to achieve the type of data archival that customer desires including CloudWatch Logs, Amazon S3, Amazon Glacier, Amazon Kinesis, and Amazon RedShift. InfoReliance will implement a data archival process for customer that focuses on 3 separate areas: Logs, Database, and Static Content.
SW license management	Manage software and OS software licensing. Also manage database licensing for RDS.
Full lifecycle cloud application development, migration, and support	Provide requirements, design, development, test, migration, and support for cloud workloads and software applications based on a CMMI, ISO, and ITIL proven framework and methodology.
Big Data and analytics	Design, configure, and support big data IaaS services to include EMR and Hadoop managed services. Also includes access to expert data scientists and analysts as required.
Consulting services	Provide full lifecycle consulting services to include requirements gathering, detailed design, expert implementation, and dedicated ongoing support to subject matter experts as required and managed by dedicated project and program managers.
Systems engineering and configuration services	Perform systems engineering and configuration services for cloud implementations and through the iFRAME SDLC framework and quality processes.
O365 mailbox migration with email, collaboration, and instant messaging	Leverage the extensive experience and expertise deploying, migrating, and supporting over 125,000 users into O365 for public sector customers and over \$200M in awarded O365 multi-year contracts.

Cloud Migration Framework: For optional services, InfoReliance proposes the use of our customizable Cloud Migration Framework (**Figure 21**). This approach provides customer with an engineering framework and foundation for complete cloud migration and cutover for any number of applications.

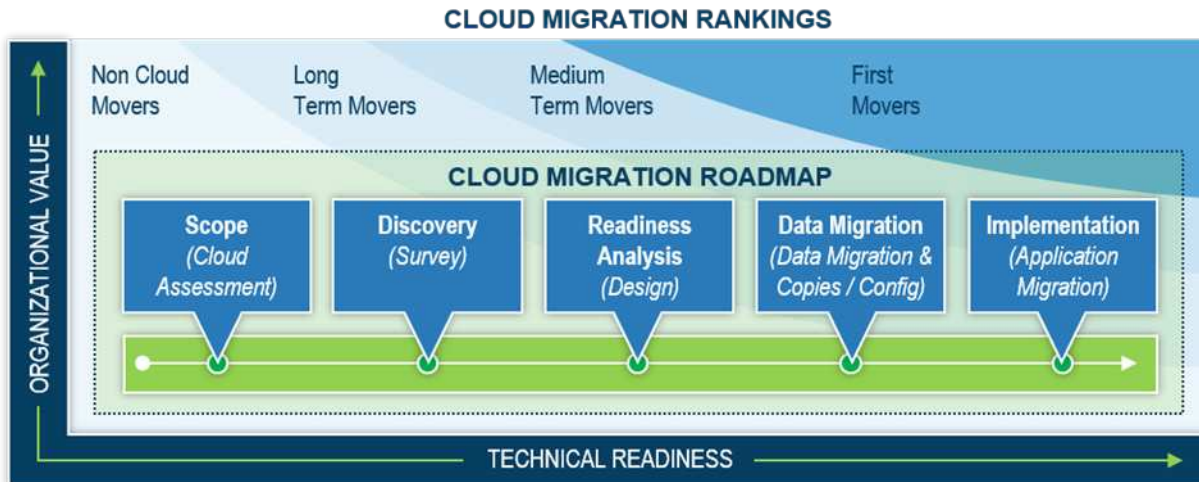


Figure 21: InfoReliance Cloud Migration Framework. InfoReliance uses a proven, structured framework to schedule, plan, and conduct migrations of customer applications to the cloud.

- ▶ **Strategy Selection:** Our selection of a specific strategy to migrate an application utilizes our Cloud Managed Services team to analyze and assess an organization's business objectives and technical processes. This process helps us build a complete recommendation to the optimal architecture design, provisioning methods, and use of orchestration and automation procedures that leverage native AWS and third-party capabilities. The automation and orchestration capabilities include scaling responses to current environment metrics such as usage or time of day, orchestrated responses to incidents, self-healing architectures, automated monitoring and performance reporting, and standardized deployment and provisioning. The ultimate goal of the designed architecture is to maximize the use of available cloud services, reduce the need for manual intervention or actions, and increase the overall reliability, security, and performance of the environment. Our solutions include both the technical implementation as well as documented processes for utilizing the tools and frameworks provided.
- ▶ **Scope:** InfoReliance will work with customer to take an inventory of applications and services that have already been chosen to be migrated to the cloud. Using our business, technical, and security and compliance assessment criteria, we will collect metadata about these applications including business criticality, stakeholders, underlying technologies, risks, and dependencies. These factors will produce a cloud readiness score for each application from rating its technical readiness to move to the cloud and the business value derived from moving.
- ▶ **Discovery:** Once the initial scope is determined, InfoReliance will perform additional discovery to ensure external dependencies, processes, and technical requirements about the scoped applications are captured and considered. An additional survey to discover and analyze other business applications that could be candidates for cloud migration following the process as the Scope phase. This will identify other factors that may impact the cloud migration roadmap and design stages.
- ▶ **Readiness Analysis:** During this stage, we will group applications using their cloud readiness scores which will provide customer with a Cloud Migration Ranking graph with each application falling into either First Movers, Medium Term Movers, Long Term Movers, or Non Cloud Movers. This ranking will help InfoReliance in developing an efficient application migration strategy and roadmap. Each application will be analyzed to ensure

the correct migration strategy is chosen and ensure application integrity post migration. Examples of factors that will be assessed for readiness and pace of migration include the Operating System mapping, stakeholder approval, maintenance window size, maintenance window frequency, architecture documentation, architecture complexity, internal/external integration points, Virtual Machine (VM) dependencies, non-VM components, data locations, security complexity, and network connectivity

- ▶ **Data Migration:** In order to prepare for an application's migration, the data it utilizes will need to be made available in the cloud environment, such as install media, configuration files, static content, and a database copy to synchronize with the existing environment. During this stage, InfoReliance will also design and build the appropriate cloud networking, security, automation, and storage platforms required to support migrated applications.
- ▶ **Migration Tools:** InfoReliance has strategic partnerships with many of the leading cloud migration tool sets and based on the specific customer requirements the migration tool will be selected. Examples of migration tools include Racemi, Cloud Endure, Double take, and additional native AWS and open source toolsets.
- ▶ **Implementation:** During this final stage, InfoReliance will use our cloud orchestration framework to create the application stacks by building baseline templates and deployment and automation scripts. This enables quick deployment of an application, applies the most recent configuration files and data, and prepares the environment to monitor and manage new assets. The automation and deployment scripts will leverage AWS CloudFormation, OpsWorks, or Elastic Beanstalk as well as operating system specific scripting languages. These templates, scripts and configuration files will become part of the application's definition and as part of the application's source code or configuration files in Amazon S3.

To implement the cloud migration framework, InfoReliance will customize a project plan containing a detailed schedule that will account for the number of applications, complexity of the applications, and their cloud migration readiness score. Our roadmap for each application will leverage the continuum shown in **Figure 22** to determine the best strategy to maximize the effectiveness of the cloud while considering resources and time available.

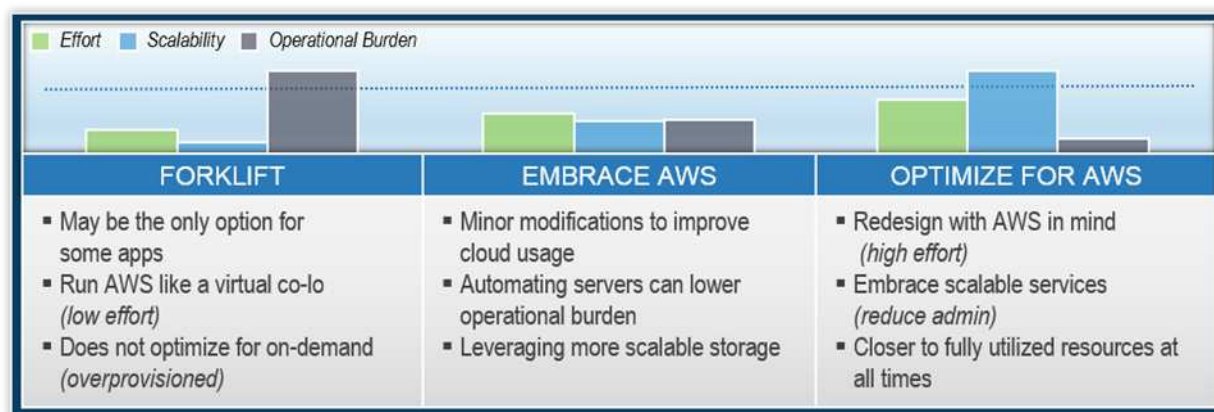


Figure 22: The AWS Migration Continuum. InfoReliance will use this continuum to select the best strategy and approach for developing each application's cloud roadmap and detailed project plan.

Proven Past Performance: As demonstrated in **Section 4.1 Business Profile** and **Section 4.2 Scope of Experience**, InfoReliance is an undisputed leader in providing cloud-based solutions and related cloud-enabling services with 30+ public sector customers. The table below summarizes key customers for both the NASPO required value-added services and the optional services that may be desired by a Participating Entity.

Key Disciplines and Services	Required /Optional	TVA	DOI	NARA	DOL	HHS	Amazon.com
BPA Management – to include meeting and decision support.	R	✓	✓	✓	✓	✓	✓
AWS IaaS	R	✓	✓	✓	✓	✓	✓
Azure IaaS	O	✓	✓		✓	✓	
Office 365	O				✓	✓	
Initial setup, provisioning, and access to the services	R	✓	✓	✓	✓	✓	✓
Provide administrative services for the cloud console and hybrid cloud environment, including cloud Single Sign On.	O	✓	✓	✓	✓	✓	✓
Cloud Infrastructure Operations	O	✓	✓	✓	✓	✓	✓
Database/application administration	O	✓	✓	✓	✓	✓	✓
Systems engineering and configuration services	O	✓	✓	✓	✓	✓	✓
AWS/Cloud Infrastructure Migration	O	✓	✓	✓	✓	✓	✓
Big Data and analytics,	O	✓	✓	✓	✓	✓	✓
Full lifecycle software development for web applications in the Cloud	O	✓	✓	✓	✓	✓	✓
Cloud consulting services	O	✓	✓	✓	✓	✓	✓
Cloud DevOps automation for continuous deployment and integration.	O	✓	✓	✓	✓	✓	✓
Disaster recovery, back up, and continuity of operations planning	O	✓	✓	✓	✓	✓	✓
24x7 cloud support center	O	✓	✓	✓	✓	✓	✓
Information Assurance / cloud security	O	✓	✓	✓	✓	✓	✓
Cloud training	R	✓	✓	✓	✓	✓	✓
O365 mailbox migration	O				✓	✓	
Email and Instant messaging	O				✓	✓	

6.22. (E) Supporting Infrastructure (RFP 8.22)

In this section, we demonstrate that our capabilities meet or exceed the RFP requirements for supporting infrastructure and should be scored **Superior**.

6.22.1. Infrastructure Required by Purchasing Entity (RFP 8.22.1)

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

The only infrastructure required by a Participating Entity to leverage most AWS services is connectivity via internet, VPN, or Direct Connect and a supported web browser.

6.22.2. Responsibility for Installation of New Infrastructure (RFP 8.22.2)

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

Each Participating Entity is responsible for installation of new infrastructure on their on-premises environment and they will be responsible for costs associated with that. Any infrastructure on the AWS is installed by AWS.

6.23. (E) 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).

As described in **Section 6.1.2** AWS cloud services meet and exceed the requirement to align with NIST Cloud Computing Reference Architecture as it relates to IaaS and should be scored **Superior**. AWS offers all of its services with the premise that a Participating Entity will be able to directly access, provision, and manage the cloud services AWS provides.



Amazon Web Services: Risk and Compliance

December 2015

(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	3
<i>Shared Responsibility Environment</i>	<i>3</i>
<i>Strong Compliance Governance</i>	<i>4</i>
Evaluating and Integrating AWS Controls	4
<i>AWS IT Control Information</i>	<i>5</i>
<i>AWS Global Regions</i>	<i>5</i>
AWS Risk and Compliance Program	6
<i>Risk Management</i>	<i>6</i>
<i>Control Environment</i>	<i>6</i>
<i>Information Security</i>	<i>7</i>
AWS Certifications, Programs, Reports, and Third-Party Attestations	7
<i>CJIS</i>	<i>7</i>
<i>CSA</i>	<i>7</i>
<i>Cyber Essentials Plus</i>	<i>8</i>
<i>DoD SRG Levels 2 and 4</i>	<i>8</i>
<i>FedRAMP SM</i>	<i>8</i>
<i>FERPA</i>	<i>9</i>
<i>FIPS 140-2</i>	<i>9</i>
<i>FISMA and DIACAP</i>	<i>9</i>
<i>HIPAA</i>	<i>10</i>
<i>IRAP</i>	<i>10</i>
<i>ISO 9001</i>	<i>11</i>
<i>ISO 27001</i>	<i>12</i>
<i>ISO 27017</i>	<i>13</i>
<i>ISO 27018</i>	<i>14</i>
<i>ITAR</i>	<i>15</i>
<i>MPAA</i>	<i>15</i>
<i>MTCS Tier 3 Certification</i>	<i>16</i>
<i>NIST</i>	<i>16</i>

<i>PCI DSS Level 1</i>	16
<i>SOC 1/ISAE 3402</i>	17
<i>SOC 2</i>	19
<i>SOC 3</i>	19
<i>Key Compliance Questions and AWS</i>	19
AWS Contact	24
Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1	25
Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations	62
Appendix C: Glossary of Terms	82

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/): <https://aws.amazon.com/security/>

For a more detailed description of AWS Compliance please see

[AWS Compliance page](https://aws.amazon.com/compliance/): <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 eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), 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: \[http://iase.disa.mil/cloud_security/Pages/index.aspx\]\(http://iase.disa.mil/cloud_security/Pages/index.aspx\)](#).

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 FedRAMPsm compliance please see the [AWS FedRAMPsm 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](#)).

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 assessment](#) 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://do.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://do.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://do.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](https://aws.amazon.com/compliance/mpaa/) 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.
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 sm), 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.

Ref	Cloud Computing Question	AWS Information
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 eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), 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 sm 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.
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 FedRAMP sm 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.

Ref	Cloud Computing Question	AWS Information
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.
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.

Ref	Cloud Computing Question	AWS Information
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.
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.

Ref	Cloud Computing Question	AWS Information
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 <i>Application Security</i>	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 <i>Customer Access Requirements</i>	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 <i>Data Integrity</i>	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 <i>Data Security / Integrity</i>	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 <i>Audit Planning</i>	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 <i>Independent Audits</i>	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.
	AAC - 02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	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 - 02.6	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 <i>Information System Regulatory Mapping</i>	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
	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 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. 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 eleven regions: 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), 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 <i>Business Continuity Planning</i>	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 <i>Business Continuity Testing</i>	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 <i>Power / Telecommunications</i>	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 <i>Environmental Risks</i>	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 <i>Equipment Location</i>	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 <i>Equipment Maintenance</i>	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 <i>Equipment Power Failures</i>	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 <i>Impact Analysis</i>	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 <i>Policy</i>	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 <i>Retention Policy</i>	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/. 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-11.2	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?	
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	
Change Control & Configuration Management <i>New Development / Acquisition</i>	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 <i>Outsourced Development</i>	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.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	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 <i>Quality Testing</i>	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/ .
	CCC-03.2	Is documentation describing known issues with certain products/services available?	AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com .
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	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.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	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.
Change Control & Configuration Management <i>Unauthorized Software Installations</i>	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 <i>Production Changes</i>	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 14 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 <i>Classification</i>	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 eleven regions: 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), 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 eleven regions: 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), China (Beijing) Region and South America (Sao Paulo).
Data Security & Information Lifecycle Management <i>Data Inventory / Flows</i>	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 eleven regions: 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), 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 <i>eCommerce Transactions</i>	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.
	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)?	Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
Data Security & Information Lifecycle Management <i>Handling / Labeling / Security Policy</i>	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 <i>Nonproduction Data</i>	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 <i>Ownership / Stewardship</i>	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 <i>Secure Disposal</i>	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 <i>Asset Management</i>	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 <i>Controlled Access Points</i>	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 <i>Equipment Identification</i>	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 <i>Offsite Authorization</i>	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 <i>Offsite equipment</i>	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 <i>Policy</i>	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 <i>Secure Area Authorization</i>	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 eleven regions: 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), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security <i>Unauthorized Persons Entry</i>	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.
Datacenter Security <i>User Access</i>	DCS -09.1	Do you restrict physical access to information assets and functions by users and support personnel?	AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Encryption & Key Management <i>Entitlement</i>	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 <i>Key Generation</i>	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/).
	EKM -02.2	Do you have a capability to manage encryption keys on behalf of tenants?	Refer to AWS SOC reports for more details on KMS.
	EKM -02.3	Do you maintain key management procedures?	In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
	EKM -02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	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.
	EKM -02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
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.
	EKM - 04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	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.
	EKM - 04.3	Do you store encryption keys in the cloud?	
	EKM - 04.4	Do you have separate key management and key usage duties?	AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Governance and Risk Management Baseline Requirements	GR M- 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.
	GR M- 01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GR M- 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 <i>Risk Assessments</i>	GR M-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.
	GR M-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 <i>Management Oversight</i>	GR M-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 <i>Management Program</i>	GR M-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/ .
	GR M-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	
Governance and Risk Management <i>Management Support / Involvement</i>	GR M-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).
Governance and Risk Management <i>Policy</i>	GR M-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external

Control Group	CID	Consensus Assessment Questions	AWS Response
	GR M-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/.
	GR M-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GR M-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management <i>Policy Enforcement</i>	GR M-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.
	GR M-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	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.
Governance and Risk Management <i>Business / Policy Change Impacts</i>	GR M-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 <i>Policy Reviews</i>	GR M-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.
	GR M-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 <i>Assessments</i>	GR M-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
	GR M-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	GR M-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.
	GR M-11.2	Do you make available documentation of your organization-wide risk management program?	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.
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.
	HRS -03.2	Do you document employee acknowledgment of training they have completed?	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 -03.3	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 <i>Employment Termination</i>	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 <i>Portable / Mobile Devices</i>	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 <i>Nondisclosure Agreements</i>	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 <i>Roles / Responsibilities</i>	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 <i>Acceptable Use</i>	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 <i>Training / Awareness</i>	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 <i>User Responsibility</i>	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 <i>Workspace</i>	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 <i>Audit Tools Access</i>	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 <i>User Access Policy</i>	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 <i>Diagnostic / Configuration Ports Access</i>	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 <i>Policies and Procedures</i>	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 <i>Segregation of Duties</i>	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 6.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management <i>Source Code Access Restriction</i>	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 <i>Third Party Access</i>	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 <i>User Access Restriction / Authorization</i>	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 <i>User Access Authorization</i>	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 <i>User Access Reviews</i>	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 <i>User Access Revocation</i>	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 <i>User ID Credentials</i>	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?	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 -12.7	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?	
	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 <i>Utility Programs Access</i>	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 <i>Audit Logging / Intrusion Detection</i>	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) have 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.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	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 .
Infrastructure & Virtualization Security <i>Change Detection</i>	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 <i>Clock Synchronization</i>	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.
	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 <i>Management - Vulnerability Management</i>	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 <i>Network Security</i>	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.
	IVS-06.4	Are all firewall access control lists documented with business justification?	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.
Infrastructure & Virtualization Security <i>OS Hardening and Base Controls</i>	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?	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-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/ .
Infrastructure & Virtualization Security <i>Production / Nonproduction Environments</i>	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 <i>Segmentation</i>	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 <i>VM Security - vMotion Data Protection</i>	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 <i>VMM Security - Hypervisor Hardening</i>	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 <i>Wireless Security</i>	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 <i>Network Architecture</i>	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.
Interoperability & Portability <i>Data Request</i>	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Interoperability & Portability <i>Policy & Legal</i>	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 <i>Standardized Network Protocols</i>	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 <i>Virtualization</i>	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 <i>Anti-Malware</i>	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 <i>Application Stores</i>	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).
Mobile Security <i>Approved Applications</i>	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 <i>Approved Software for BYOD</i>	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 <i>Awareness and Training</i>	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 <i>Cloud Based Services</i>	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 <i>Compatibility</i>	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security <i>Device Eligibility</i>	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security <i>Device Inventory</i>	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 <i>Device Management</i>	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 <i>Encryption</i>	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 <i>Jailbreaking and Rooting</i>	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?	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 <i>Legal</i>	MOS -13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	
	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 <i>Lockout Screen</i>	MOS -14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security <i>Operating Systems</i>	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 <i>Passwords</i>	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 <i>Policy</i>	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 <i>Remote Wipe</i>	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 <i>Security Patches</i>	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 <i>Users</i>	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	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. AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The AWS SOC reports provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities.
	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 <i>Contact / Authority Maintenance</i>	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	
	SEF-02.1	Do you have a documented security incident response plan?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Incident Management</i>	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?	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 <i>Incident Reporting</i>	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 <i>Incident Response Legal Preparation</i>	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 <i>Incident Response Metrics</i>	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	
	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 <i>Data Quality and Integrity</i>	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 <i>Incident Reporting</i>	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 <i>Network / Infrastructure Services</i>	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 <i>Provider Internal Assessments</i>	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 8 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 <i>Third Party Agreements</i>	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 <i>Supply Chain Governance Reviews</i>	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 <i>Supply Chain Metrics</i>	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 <i>Third Party Assessment</i>	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 <i>Third Party Audits</i>	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 <i>Antivirus / Malicious Software</i>	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 <i>Vulnerability / Patch Management</i>	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 <i>Mobile Code</i>	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. 2 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 9.1 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. 2 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 and 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 FedRAMPsm.
	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 12.2 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 99.99999999% 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 web servers 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 FedRAMPsm. 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 FedRAMPsm.
	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 9.1 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 7.1 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 9.1 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?	The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution. 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.
	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.

FedRAMPsm: The Federal Risk and Authorization Management Program (FedRAMPsm) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMPsm 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 users 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

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: FedRAMPsm, 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

© 2010-2016 Amazon.com, Inc., or its affiliates. This document is provided for informational purposes only. It represents AWS' current product offerings as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

PRODUCTS & SERVICES[Amazon EC2](#) >[Product Details](#) >[Instances](#) >[Pricing](#) >[Purchasing Options](#) >[Developer Resources](#) >[FAQs](#) >[Getting Started](#) >[Amazon EC2 Run Command](#) >

RELATED LINKS

[Amazon EC2 Dedicated Hosts](#)[Amazon EC2 Spot Instances](#)[Amazon EC2 Reserved Instances](#)[Amazon EC2 Dedicated Instances](#)[Windows Instances](#)[VM Import/Export](#)[AWS Management](#)

Amazon EC2 Service Level Agreement

Last Updated June 1, 2013

This Amazon EC2 Service Level Agreement (“SLA”) is a policy governing the use of Amazon Elastic Compute Cloud (“Amazon EC2”) and Amazon Elastic Block Store (“Amazon EBS”) under the terms of the Amazon Web Services Customer Agreement (the “AWS Agreement”) between Amazon Web Services, Inc. and its affiliates (“AWS”, “us” or “we”) and users of AWS’ services (“you”). This SLA applies separately to each account using Amazon EC2 or Amazon EBS. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon EC2 and Amazon EBS each available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the “Service Commitment”). In the event Amazon EC2 or Amazon EBS does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- “Monthly Uptime Percentage” is calculated by subtracting from 100% the percentage of minutes during the month in which Amazon EC2 or Amazon EBS, as applicable, was in the state of “Region Unavailable.” Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon EC2 SLA Exclusion (defined below).
- “Region Unavailable” and “Region Unavailability” mean that more than one Availability Zone in which you are running an instance, within the

same Region, is “Unavailable” to you.

- “Unavailable” and “Unavailability” mean:
 - For Amazon EC2, when all of your running instances have no external connectivity.
 - For Amazon EBS, when all of your attached volumes perform zero read write IO, with pending IO in the queue.
- A “Service Credit” is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

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%

We will apply any Service Credits only against future Amazon EC2 or Amazon EBS payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon EC2 or Amazon EBS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by [opening a case in the AWS Support Center](#). To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

1. the words “SLA Credit Request” in the subject line;
2. the dates and times of each Unavailability incident that you are claiming;
3. the affected EC2 instance IDs or the affected EBS volume IDs; and
4. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon EC2 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2 or Amazon EBS, or any other Amazon EC2 or Amazon EBS performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2 or Amazon EBS; (iii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances or volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the AWS Agreement; or (vii) arising from our suspension and termination of your right to use Amazon EC2 or Amazon EBS in accordance with the AWS Agreement (collectively, the “Amazon EC2 SLA Exclusions”). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

[Prior Version\(s\)](#)[Create a Free Account](#)[AWS on Twitter](#)[f AWS on Facebook](#)[g+ AWS on Google+](#)[AWS Blog](#)[What's New? RSS](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)[Products & Services](#)[Customer Success](#)[Economics Center](#)[Architecture Center](#)[Security Center](#)[What's New](#)[Whitepapers](#)[AWS Blog](#)[Events](#)[Sustainable Energy](#)[Press Releases](#)[Analyst Reports](#)[Legal](#)

Solutions

[Websites & Website Hosting](#)[Business Applications](#)[Backup & Recovery](#)[Disaster Recovery](#)[Data Archive](#)[Big Data](#)[High Performance Computing](#)[Mobile Services](#)[Digital Marketing](#)[Game Development](#)[Digital Media](#)[Government & Education](#)

Resources & Training

[Developers](#)[Java on AWS](#)[JavaScript on AWS](#)[Mobile on AWS](#)[PHP on AWS](#)[Python on AWS](#)[Ruby on AWS](#)[Windows & .NET on AWS](#)[SDKs & Tools](#)[AWS Marketplace](#)[User Groups](#)[Support Plans](#)[Service Health Dashboard](#)[Discussion Forums](#)[FAQs](#)[Documentation](#)[Articles & Tutorials](#)[Test Drives](#)

Manage Your Account

[Management Console](#)[Billing & Cost Management](#)[Personal Information](#)[Payment Method](#)[AWS Identity & Access Management](#)[Security Credentials](#)[Request Service Limit Increases](#)[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [Careers](#) page or our [Developer-specific Careers](#) page to learn more.

Amazon Web Services is an Equal Opportunity Employer.

An  **amazon** company.

Language [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [Português](#) | [Русский](#) | [日本語](#) | [한국어](#) | [中文 \(简体\)](#) | [中文 \(繁體\)](#)

[Site Terms](#) | [Privacy](#)

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.



PRODUCTS & SERVICES

[Amazon S3](#) >[Storage Classes](#) >[Pricing](#) >[Getting Started](#) >[Resources](#) >[Product Details](#) >[FAQs](#) >[Amazon S3 SLA](#) >

RELATED LINKS

[AWS Management Console](#)[Documentation](#)[Release Notes](#)[Discussion Forum](#)

Amazon S3 Service Level Agreement

[Create Free Account »](#)

Last Updated September 16, 2015

This Amazon S3 Service Level Agreement (“SLA”) is a policy governing the use of Amazon Simple Storage Service (“Amazon S3”) under the terms of the Amazon Web Services Customer Agreement (the “AWS Agreement”) between Amazon Web Services, Inc. and its affiliates (“AWS”, “us” or “we”) and users of AWS’ services (“you”). This SLA applies separately to each account using Amazon S3. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon S3 available with the applicable Monthly Uptime Percentage (as defined below) during any monthly billing cycle (the “Service Commitment”). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- “Error Rate” means: (i) the total number of internal server errors returned by Amazon S3 as error status “InternalError” or “ServiceUnavailable” divided by (ii) the total number of requests for the applicable request type during that five minute period. We will calculate the Error Rate for each Amazon S3 account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions (as defined below).
- “Monthly Uptime Percentage” is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly

billing cycle.

- A “Service Credit” is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon S3 account.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below.

For all requests not otherwise specified below:

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99.0% but less than 99.9%	10%
Less than 99.0%	25%

For requests to Amazon S3 Standard – Infrequent Access (Standard-IA):

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 98.0% but less than 99.0%	10%
Less than 98.0%	25%

We will apply any Service Credits only against future Amazon S3 payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by

us to provide Amazon S3 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by [opening a case in the AWS Support Center](#). To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

1. the words “SLA Credit Request” in the subject line;
2. the dates and times of each incident of non-zero Error Rates that you are claiming; and
3. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than the applicable Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the “Amazon S3 SLA Exclusions”). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.

[Prior Version\(s\)](#)[Create a Free Account](#)

 [AWS on Twitter](#)  [AWS on Facebook](#)  [AWS on Google+](#)  [AWS Blog](#)
 [What's New? RSS](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)[Products & Services](#)[Customer Success](#)[Economics Center](#)[Architecture Center](#)[Security Center](#)[What's New](#)[Whitepapers](#)[AWS Blog](#)[Events](#)[Sustainable Energy](#)[Press Releases](#)[Analyst Reports](#)[Legal](#)

Solutions

[Websites & Website Hosting](#)[Business Applications](#)[Backup & Recovery](#)[Disaster Recovery](#)[Data Archive](#)[Big Data](#)[High Performance Computing](#)[Mobile Services](#)[Digital Marketing](#)[Game Development](#)[Digital Media](#)[Government & Education](#)

Resources & Training

[Developers](#)

[Java on AWS](#)
[JavaScript on AWS](#)
[Mobile on AWS](#)
[PHP on AWS](#)
[Python on AWS](#)
[Ruby on AWS](#)
[Windows & .NET on AWS](#)
[SDKs & Tools](#)
[AWS Marketplace](#)
[User Groups](#)
[Support Plans](#)
[Service Health Dashboard](#)
[Discussion Forums](#)
[FAQs](#)
[Documentation](#)
[Articles & Tutorials](#)
[Test Drives](#)

Manage Your Account

[Management Console](#)
[Billing & Cost Management](#)
[Personal Information](#)
[Payment Method](#)
[AWS Identity & Access Management](#)
[Security Credentials](#)
[Request Service Limit Increases](#)
[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [Careers](#) page or our [Developer-specific Careers](#) page to learn more.

Amazon Web Services is an Equal Opportunity Employer.

Language [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [Português](#) | [Русский](#) | [日本語](#) | [한국어](#) | [中文 \(简体\)](#)
[中文 \(繁體\)](#)

[Site Terms](#) | [Privacy](#)

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.



PRODUCTS & SERVICES

[Amazon CloudFront](#) >[Product Details](#) >[Dynamic Content Delivery](#) >[Reports & Analytics](#) >[Media Streaming Tutorials](#) >[Pricing](#) >[Getting Started](#) >[Developer Resources](#) >[CloudFront SLA](#) >[What's New?](#) >[Amazon CloudFront Events](#) >[FAQs](#) >[Webinars & Videos](#) >

RELATED LINKS

[Documentation](#)[AWS Management Console](#)

Amazon CloudFront Service Level Agreement

Last Updated June 1, 2013

This Amazon CloudFront Service Level Agreement (“**SLA**”) is a policy governing the use of Amazon CloudFront under the terms of the Amazon Web Services Customer Agreement (the “**AWS Agreement**”) between Amazon Web Services, Inc. and its affiliates (“**AWS**”, “**us**” or “**we**”) and users of AWS’ services (“**you**”). This SLA applies separately to each account using Amazon CloudFront. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement

Service Commitment

AWS will use commercially reasonable efforts to make Amazon CloudFront available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the “**Service Commitment**”). In the event Amazon CloudFront does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- “**Error Rate**” means: (i) the total number of internal server errors returned by Amazon CloudFront divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon CloudFront account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon CloudFront SLA Exclusions (as defined below).
- “**Monthly Uptime Percentage**” is calculated by subtracting from 100%

[Release Notes](#)[Discussion Forums](#)

the average of the Error Rates from each five minute period in the monthly billing cycle.

- A “**Service Credit**” is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon CloudFront for the billing cycle in which the error occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon CloudFront payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon CloudFront is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by [opening a case in the AWS Support Center](#). To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

- i. the words “SLA Credit Request” in the subject line;
- ii. the dates and times of each incident of non-zero Error Rates that you are claiming; and
- iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon CloudFront SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon CloudFront, or any other Amazon CloudFront performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon CloudFront; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon CloudFront in accordance with the AWS Agreement; (vi) that result from exceeding usage limits stated in the Amazon CloudFront documentation; or (vii) that result from use of an origin server other than Amazon S3 (collectively, the **“Amazon CloudFront SLA Exclusions”**). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.

[Prior Version\(s\)](#)

[Create a Free Account](#)

-  [AWS on Twitter](#)
-  [AWS on Facebook](#)
-  [AWS on Google+](#)
-  [AWS Blog](#)
-  [What's New? RSS](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)[Products & Services](#)[Customer Success](#)[Economics Center](#)[Architecture Center](#)[Security Center](#)[What's New](#)[Whitepapers](#)[AWS Blog](#)[Events](#)[Sustainable Energy](#)[Press Releases](#)[Analyst Reports](#)[Legal](#)

Solutions

[Websites & Website Hosting](#)[Business Applications](#)[Backup & Recovery](#)[Disaster Recovery](#)[Data Archive](#)[Big Data](#)[High Performance Computing](#)[Mobile Services](#)[Digital Marketing](#)[Game Development](#)[Digital Media](#)[Government & Education](#)

Resources & Training

[Developers](#)[Java on AWS](#)[JavaScript on AWS](#)[Mobile on AWS](#)[PHP on AWS](#)[Python on AWS](#)

[Ruby on AWS](#)[Windows & .NET on AWS](#)[SDKs & Tools](#)[AWS Marketplace](#)[User Groups](#)[Support Plans](#)[Service Health Dashboard](#)[Discussion Forums](#)[FAQs](#)[Documentation](#)[Articles & Tutorials](#)[Test Drives](#)

Manage Your Account

[Management Console](#)[Billing & Cost Management](#)[Personal Information](#)[Payment Method](#)[AWS Identity & Access Management](#)[Security Credentials](#)[Request Service Limit Increases](#)[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [Careers](#) page or our [Developer-specific Careers](#) page to learn more.

Amazon Web Services is an Equal Opportunity Employer.

Language [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [Português](#) | [Русский](#) | [日本語](#) | [한국어](#) | [中文 \(简体\)](#)
[中文 \(繁體\)](#)

[Site Terms](#) | [Privacy](#)

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.



PRODUCTS & SERVICES

[Amazon Route 53](#) >[Product Details](#) >[Pricing](#) >[Developer Resources](#) >[FAQs](#) >[Amazon Route 53 SLA](#) >[Amazon Route 53 Amazon Registrar Policies](#) >

RELATED LINKS

[Documentation](#)[Management Console](#)[Release Notes](#)[Discussion Forum](#)[Introduction to Amazon Route 53](#)

Amazon Route 53 Service Level Agreement

[Create Free Account »](#)

Last Updated May 15, 2015

This Amazon Route 53 Service Level Agreement (“**SLA**”) is a policy governing the use of Amazon Route 53 (including Private DNS) under the terms of the Amazon Web Services Customer Agreement (the “**AWS Agreement**”) between Amazon Web Services, Inc. and its affiliates (“**AWS**”, “**us**” or “**we**”) and users of AWS’ services (“**you**”). This SLA applies separately to each account using Amazon Route 53. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon Route 53 100% Available (defined below). In the event Amazon Route 53 does not meet the foregoing commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- “**100% Available**” means that Amazon Route 53 did not fail to respond to your DNS queries during a monthly billing cycle.
- A “**Service Credit**” is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon Route 53 account.

Service Credits

Service Credits are calculated based on 1 day of Service Credit, which is equal to your average daily Amazon Route 53 query charges for the monthly billing cycle preceding the monthly billing cycle in which the period that Amazon Route 53 was not 100% Available occurred, and are available as follows:

Duration Amazon Route 53 was not 100%**Available****Service Credit**

5 - 30 minutes	1 day Service Credit
31 minutes - 4 hours	7 days Service Credit
More than 4 hours	30 days Service Credit

We will apply any Service Credits only against future Amazon Route 53 payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon Route 53 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by [opening a case in the AWS Support Center](#). To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

- i. the words “SLA Credit Request” in the subject line;
- ii. the dates and times of each period that Amazon Route 53 was not 100% Available that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the period that Amazon Route 53 was not 100% Available is confirmed by us, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon Route 53 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon Route 53, or any other Amazon Route 53 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of Amazon Route 53's reasonable control, including any force majeure event, denial-of-service attack or Internet access or related problems beyond the demarcation point of Amazon Route 53; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon Route 53 in accordance with the AWS Agreement; (vi) that result from you exceeding usage limits stated in the Amazon Route 53 documentation (collectively, the **"Amazon Route 53 SLA Exclusions"**); or (vii) that, with respect to public DNS only, result during a period that you were not using all four virtual name servers (for example, ns123.awsdns.com, ns123.awsdns.net, ns123.awsdns.co.uk and ns123.awsdns.org) assigned to your "hosted zone". If availability is impacted by factors other than those used in our calculation of 100% Available, then we may issue a Service Credit considering such factors at our discretion.

[Prior Version\(s\)](#)

-  [AWS on Twitter](#)
-  [AWS on Facebook](#)
-  [AWS on Google+](#)
-  [AWS Blog](#)
-  [What's New? RSS](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)

[Products & Services](#)

[Customer Success](#)

[Economics Center](#)

[Architecture Center](#)

[Security Center](#)

[What's New](#)

[Whitepapers](#)

[AWS Blog](#)

[Events](#)

[Sustainable Energy](#)

[Press Releases](#)

[Analyst Reports](#)

[Legal](#)

Solutions

[Websites & Website Hosting](#)

[Business Applications](#)

[Backup & Recovery](#)

[Disaster Recovery](#)

[Data Archive](#)

[Big Data](#)

[High Performance Computing](#)

[Mobile Services](#)

[Digital Marketing](#)

[Game Development](#)

[Digital Media](#)

[Government & Education](#)

Resources & Training

[Developers](#)

[Java on AWS](#)

[JavaScript on AWS](#)

[Mobile on AWS](#)

[PHP on AWS](#)

[Python on AWS](#)

[Ruby on AWS](#)

[Windows & .NET on AWS](#)[SDKs & Tools](#)[AWS Marketplace](#)[User Groups](#)[Support Plans](#)[Service Health Dashboard](#)[Discussion Forums](#)[FAQs](#)[Documentation](#)[Articles & Tutorials](#)[Test Drives](#)

Manage Your Account

[Management Console](#)[Billing & Cost Management](#)[Personal Information](#)[Payment Method](#)[AWS Identity & Access Management](#)[Security Credentials](#)[Request Service Limit Increases](#)[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [Careers](#) page or our [Developer-specific Careers](#) page to learn more.

Amazon Web Services is an Equal Opportunity Employer.

Language [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [Português](#) | [Русский](#) | [日本語](#) | [한국어](#) | [中文 \(简体\)](#) | [中文 \(繁體\)](#)

[Site Terms](#) | [Privacy](#)

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.



PRODUCTS & SERVICES

[Amazon RDS](#) >[Product Details](#) >[Reserved
Instances](#) >[Pricing](#) >[Previous
Generation
Instances](#) >[Partners](#) >[Getting Started](#) >[Developer
Resources](#) >[FAQs](#) >[What's New](#) >[Amazon RDS SLA](#) >[Customer
Highlights](#) >

RELATED LINKS

[Amazon RDS for
Aurora](#)[Amazon RDS for
MySQL](#)[Amazon RDS for](#)

Amazon RDS Service Level Agreement

[Create Free Account »](#)

Last Updated June 1, 2013

This Amazon RDS Service Level Agreement ("SLA") is a policy governing the use of the Amazon Relational Database Service ("Amazon RDS") under the terms of the AWS Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon RDS. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Multi-AZ instances available with a Monthly Uptime Percentage (defined below) of at least 99.95% during any monthly billing cycle (the "Service Commitment"). In the event Amazon RDS does not meet the Monthly Uptime Percentage commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Monthly Uptime Percentage" for a given Multi-AZ instance is calculated by subtracting from 100% the percentage of 1 minute periods during the monthly billing cycle in which the Multi-AZ instance was "Unavailable". If you have been running that Multi-AZ instance for only part of the month, your Multi-AZ instance is assumed to be 100% available for the portion of the month that it was not running. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon RDS SLA Exclusion (defined below).

[MariaDB](#)[Amazon RDS for PostgreSQL](#)[Amazon RDS for Oracle](#)[Amazon RDS for SQL Server](#)[Management Console](#)[Release Notes](#)[Community Forum](#)[Documentation](#)

- "Multi-AZ instance" means an Amazon RDS for MySQL, Oracle or PostgreSQL database instance with the Multi-AZ parameter set to true.
- "Unavailable" means that all connection requests to the running Multi-AZ instance fail during a 1 minute period.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Credits

Service Credits are calculated as a percentage of the charges paid by you for the Multi-AZ instances that did not meet the Monthly Uptime Percentage commitment in a billing cycle 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%	25%

We will apply any Service Credits only against future Amazon RDS payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance or other failure by us to provide Amazon RDS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you will need to submit a claim by [opening a case in the AWS Support Center](#). To be eligible, the credit request must be

received by us by the end of the second billing cycle after which the incident occurred and must include:

- i. the words "SLA Credit Request" in the subject line;
- ii. the dates and times of each Unavailability incident you are claiming;
- iii. the DB Instance IDs and the AWS Regions of the affected Multi-AZ instances; and
- iv. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which the request occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon RDS SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon RDS, or any other Amazon RDS performance issues:

- (i) that result from a suspension described in Section 6.1 of the AWS Agreement;
- (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon RDS;
- (iii) that result from any voluntary actions or inactions from you or any third party (e.g., rebooting a database instance, scaling compute capacity, not scaling storage when the storage is full, misconfiguring security groups, VPC configurations or credential settings, disabling encryption keys or making the encryption keys inaccessible, etc.);
- (iv) that result from instances belonging to the Micro DB instance class or other instance classes which have similar CPU and memory resource limitations;
- (v) that result from you not following the [basic operational guidelines](#)   described in the Amazon RDS User Guide (e.g., overloading a database instance to the point it is inoperable, creating excessively large number of tables that significantly increase the recovery time etc.);

- (vi) caused by underlying database engine software that lead to repeated database crashes or an inoperable database instance;
- (vii) that result in long recovery time due to insufficient IO capacity for your database workload;
- (viii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or
- (ix) that result from any maintenance as provided for pursuant to the AWS Agreement; or
- (x) arising from our suspension and termination of your right to use Amazon RDS in accordance with the AWS Agreement (collectively, the "Amazon RDS SLA Exclusions").

If availability is impacted by factors other than those explicitly used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

[Prior Version\(s\)](#)

[Create a Free Account](#)

[AWS on Twitter](#)
[What's New? RSS](#)

[AWS on Facebook](#)

[AWS on Google+](#)

[AWS Blog](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)

[Products & Services](#)

[Customer Success](#)

[Economics Center](#)

[Architecture Center](#)

[Security Center](#)

[What's New](#)

[Whitepapers](#)

[AWS Blog](#)

[Events](#)[Sustainable Energy](#)[Press Releases](#)[Analyst Reports](#)[Legal](#)**Solutions**[Websites & Website Hosting](#)[Business Applications](#)[Backup & Recovery](#)[Disaster Recovery](#)[Data Archive](#)[Big Data](#)[High Performance Computing](#)[Mobile Services](#)[Digital Marketing](#)[Game Development](#)[Digital Media](#)[Government & Education](#)**Resources & Training**[Developers](#)[Java on AWS](#)[JavaScript on AWS](#)[Mobile on AWS](#)[PHP on AWS](#)[Python on AWS](#)[Ruby on AWS](#)[Windows & .NET on AWS](#)[SDKs & Tools](#)[AWS Marketplace](#)[User Groups](#)[Support Plans](#)[Service Health Dashboard](#)[Discussion Forums](#)[FAQs](#)[Documentation](#)[Articles & Tutorials](#)[Test Drives](#)**Manage Your Account**[Management Console](#)[Billing & Cost Management](#)

[Personal Information](#)[Payment Method](#)[AWS Identity & Access Management](#)[Security Credentials](#)[Request Service Limit Increases](#)[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [Careers](#) page or our [Developer-specific Careers](#) page to learn more.

Amazon Web Services is an Equal Opportunity Employer.

Language [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [Português](#) | [Русский](#) | [日本語](#) | [한국어](#) | [中文 \(简体\)](#) | [中文 \(繁體\)](#)

[Site Terms](#) | [Privacy](#)

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.



March 7, 2016

InfoReliance Corporation

Re: Letter of Support for NASPO ValuePoint Cloud Solutions Solicitation No. CH16012

To Whom it May Concern,

Amazon Web Services, Inc. (AWS) is very pleased to support InfoReliance Corporation in its efforts to respond to the subject pursuit using AWS cloud resources. InfoReliance Corporation is an AWS Partner Network (APN) Advanced Consulting Partner and an authorized public sector reseller.

AWS offers commercially available, web scale computing services that help organizations avoid much of the heavy-lifting typically associated with launching and growing successful applications. These services are based on Amazon's own back-end technology infrastructure and incorporate over a decade and a half of experience building one of the world's most reliable, scalable, and cost-efficient web infrastructures. The use of AWS will provide you with access to expertise in large-scale distributed computing and operations and will enable your applications to be robust and scalable.

AWS values and appreciates the opportunity to support InfoReliance Corporation and we look forward to a long and productive partnership. If you have any questions, or require additional information, please contact Jane Lacy at 703-939-5929 or jlacy@amazon.com.

Thank you,

Amazon Web Services, Inc.

A handwritten signature in black ink, appearing to read "Matthew R. Dittoe".

Signature

Name: Matt Dittoe

Title: Senior Sales Manager

Date: 3/7/2016



Certificate

Certificate number: 2013- 009

Certified by EY CertifyPoint since:

November 18, 2010



Based on certification examination in conformity with defined requirements in ISO/IEC17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

headquartered in Seattle, Washington, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: November 11, 2013

Re-issue date of certificate: December 4, 2015

Expiration date of certificate: November 12, 2016

EY CertifyPoint will, according to the certification agreement (dated October 23, 2014), perform surveillance audits and acknowledges the certificate until the expiration date of the certificate.

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in Statement of Applicability, approved on October 22, 2015.*



Drs. R. Toppen RA
Director EY CertifyPoint

Amazon Web Services, Inc.

Annex to certificate 2013- 009

The scope of this ISO 27001:2013 Certification is bounded by specified services of Amazon Web Services, Inc. and specified facilities. The ISMS is centrally managed out Amazon Web Services, Inc. headquarters in Seattle, Washington, United States of America.

The in-scope applications, systems, people, and processes are globally implemented and operated by teams out of an explicit set of facilities that comprise Amazon Web Services, Inc. and are specifically defined in the scope and bounds.

The Amazon Web Services, Inc. ISMS scope includes the following services:

- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity & Access Management (IAM)
- AWS Key Management Service (KMS)
- 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
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- VM Import/Export
- AWS WAF (Web Application Firewall)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces

Amazon Web Services, Inc.

Annex to certificate 2013- 009

Locations in scope:

- AWS Corporate Headquarters: Seattle, Washington
- Data center locations which house hardware used to deliver the services (including the Amazon GovCloud (US) region):
 - Melbourne, Australia
 - Sydney, Australia
 - Rio de Janeiro, Brazil
 - São Paulo, Brazil
 - Marseille, France
 - Paris, France
 - Frankfurt, Germany
 - Hong Kong
 - Chennai, India
 - Mumbai, India
 - Dublin, Ireland
 - Milan, Italy
 - Osaka, Japan
 - Tokyo, Japan
 - Amsterdam, Netherlands
 - Warsaw, Poland
 - Manila, Philippines
 - Singapore
 - Seoul, South Korea
 - Madrid, Spain
 - Stockholm, Sweden
 - Taipei, Taiwan
 - London, United Kingdom
 - California, United States
 - Florida, United States
 - Georgia, United States
 - Indiana, United States
 - Missouri, United States
 - New Jersey, United States
 - New York, United States
 - Oregon, United States
 - Texas, United States
 - Virginia, United States
 - Washington, United States

The ISMS mentioned in the above scope is restricted as defined in the ISMS Scope Statement, version 2015.01 approved on November 4th, 2015 by the Director of Risk & Compliance for Amazon Web Services, Inc.

AWS Service Terms

Last updated: February 22, 2016

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the [AWS Customer Agreement](#) or other agreement with us governing your use of our Services (the “Agreement”), the terms and conditions of these Service Terms apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

1. Universal Service Terms (Applicable to All Services)

1.1. You may only use the Services to store, retrieve, query, serve, and execute Your Content that is owned, licensed or lawfully obtained by you. As used in these Service Terms, “Your Content” includes any “Company Content” and any “Customer Content”. As part of the Services, you may be allowed to use certain software (including related documentation) provided by us or third party licensors. This software is neither sold nor distributed to you and you may use it solely as part of the Services. You may not transfer it outside the Services without specific authorization to do so.

1.2. You must comply with the current technical documentation applicable to the Services (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site. In addition, if you create technology that works with a Service, you must comply with the current technical documentation applicable to that Service (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site.

1.3. You will provide information or other materials related to Your Content (including copies of any client-side applications) as reasonably requested by us to verify your compliance with the Agreement. We may monitor the external interfaces (e.g., ports) of Your Content to verify your compliance with the Agreement. You will not block or interfere with our monitoring, but you may use encryption technology or firewalls to help keep Your Content confidential. You will reasonably cooperate with us to identify the source of any problem with the Services that we reasonably believe may be attributable to Your Content or any end user materials that you control.

1.4. If we reasonably believe any of Your Content violates the law, infringes or misappropriates the rights of any third party or otherwise violates a material term of the Agreement (including the documentation, the Service Terms, or the [Acceptable Use Policy](#)) (“Prohibited Content”), we will notify you of the Prohibited Content and may request that such content be removed from the Services or access to it be disabled. If you do not remove or disable access to the Prohibited Content within 2 business days of our notice, we may remove or disable access to the Prohibited Content or suspend the Services to the extent we are not able to remove or disable access to the Prohibited Content. Notwithstanding the foregoing, we may remove or disable access to any Prohibited Content without prior notice in connection with illegal content, where the

content may disrupt or threaten the Services, pursuant to the Digital Millennium Copyright Act or as required to comply with law or any judicial, regulatory or other governmental order or request. In the event that we remove content without prior notice, we will provide prompt notice to you unless prohibited by law.

1.5. From time to time, we may offer free or discounted pricing programs covering certain usage of the Services (each, a “Special Pricing Program”). We may stop accepting new sign-ups or discontinue a Special Pricing Program at any time. Standard charges will apply after a Special Pricing Program ends or if you exceed the limitations by the Special Pricing Program. You must comply with any additional terms, restrictions, or limitations (e.g., limitations on the total amount of usage) for the Special Pricing Program as described in the offer terms for the Special Pricing Program or on the pricing page for the eligible Service(s). You may not access or use the Services in a way intended to avoid any additional terms, restrictions, or limitations (e.g., establishing multiple AWS accounts in order to receive additional benefits under a Special Pricing Program), and we may immediately terminate your account if you do so. Any data stored or instances provided as part of a Special Pricing Program must be actively used.

1.6. If we make multiple discounts or pricing options for a Service available to you at one time, you will only be eligible to receive one discount or pricing option, and will not be entitled to cumulative discounting and pricing options.

1.7. You will ensure that all information you provide to us via the AWS Site (for instance, information provided in connection with your registration for the Services, requests for increased usage limits, etc.) is accurate, complete and not misleading.

1.8. From time to time, we may apply upgrades, patches, bug fixes or other maintenance to the Service Offerings (“Maintenance”). We agree to use reasonable efforts to provide you with prior notice of any scheduled Maintenance (except for emergency Maintenance) and you agree to use reasonable efforts to comply with any Maintenance requirements that we notify you about.

1.9 If your Agreement does not include a provision on AWS Confidential Information, and you and AWS do not have an effective non-disclosure agreement in place, then you agree that you will not disclose AWS Confidential Information (as defined in the AWS Customer Agreement), except as required by law.

1.10 Beta Service Participation

1.10.1. This Section describes the additional terms and conditions under which you may access and use certain features, technologies and services made available to you by AWS that are not yet generally available, including, but not limited to, any products, services, or features labeled “beta”, “preview”, “pre-release”, or “experimental” (each, a “Beta Service”) or access and use Service Offerings available in AWS regions that are not generally available, including, but not limited to, any AWS regions identified by AWS as “beta”, “preview”, “pre-release”, or “experimental” (each, a “Beta Region”). In the event there is a conflict between the terms of this Section 1.10 and an existing AWS

Beta Test Participation Agreement between you and AWS, the terms of the existing AWS Beta Test Participation Agreement will take precedence.

1.10.2. During the term of the applicable Beta Service or Beta Region (as specified by AWS), you may: (a) access and use the Beta Service or Service Offerings in any Beta Region solely for internal evaluation purposes; and (b) install, copy, and use any related AWS Content that may be provided to you by AWS in connection with the Beta Service or Service Offerings in any Beta Region (“Beta Materials”) solely as necessary to access and use the Beta Service or Service Offerings in any Beta Region in the manner permitted by this Section.

1.10.3. You agree not to allow access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials by any third party other than your employees and contractors who (i) have a need to use or access the Beta Service, Service Offerings in the Beta Region or Beta Materials in connection with your internal evaluation activities, and (ii) have executed written non-disclosure agreements obligating them to protect the confidentiality of non-public information regarding the Beta Service, Beta Region and Beta Materials.

1.10.4. You must comply with all policies and guidelines related to any Beta Service or Beta Region as posted on the AWS Site or otherwise made available to you, including the Privacy Policy, Acceptable Use Policy, the Service Terms, and any additional terms and conditions for a specific Beta Service or Beta Region. AWS may add or modify restrictions, including lowering or raising any usage limits, related to access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials at any time. If requested by AWS, you will promptly increase or decrease your usage of the applicable Beta Service, Service Offerings in a Beta Region or Beta Materials to the levels that AWS may specify. Service Level Agreements do not apply to Beta Services or any Services Offerings in Beta Regions.

1.10.5. AWS may suspend or terminate your access to or use of any Beta Service or Service Offerings in any Beta Region at any time and for any reason. AWS may at any time cease providing any or all of any Beta Service or any Service Offering in a Beta Region in its sole discretion and without notice. Beta Services and Services Offerings in Beta Regions also may be unavailable and/or their performance may be negatively affected by scheduled and unscheduled maintenance. AWS will use reasonable efforts to notify you in advance of scheduled maintenance, but AWS is unable to provide advance notice of unscheduled or emergency maintenance.

1.10.6. In consideration of being allowed to access and use a Beta Service or Service Offering in a Beta Region, you agree to provide AWS with information relating to your access, use, testing, or evaluation of the Beta Service, Service Offerings in the Beta Region or any related Beta Materials, including observations or information regarding the performance, features and functionality of the Beta Service or any related Beta Materials as applicable, when and in the form reasonably requested by AWS (“Test Observations”). AWS will own and may use and evaluate all Test Observations for its own purposes. You will not use any Test Observations except for your internal evaluation purposes of the Beta Service or Beta Region.

1.10.7. Each individual Beta Service and Service Offering in a Beta Region will automatically terminate upon the release of a generally available version of the applicable Beta Service or Service Offering in a Beta Region or upon notice of termination by AWS. Notwithstanding anything to the contrary in the Agreement or these Services Terms, either you or AWS may terminate your participation in a Beta Service or Service Offering in a Beta Region at any time for any reason upon notice to the other party. Notwithstanding anything to the contrary in the Agreement, after the conclusion of your participation in a Beta Service or Service Offering in a Beta Region for any reason, (a) you will not have any further right to access or use the applicable Beta Service or Service Offering in the Beta Region and Beta Materials; (b) your Content used in the applicable Beta Service or Service Offering in the Beta Region may be deleted or inaccessible; and (c) you will immediately return or, if instructed by AWS, destroy all Beta Materials or any other AWS Confidential Information related to the applicable Beta Service, Service Offering in any Beta Region or Beta Materials. If AWS releases a generally available version of a Beta Service or a Service Offering in a Beta Region, your access to and use of the generally available version will be subject to the Agreement and any separate Section of these Service Terms as may be specified for that generally available Service Offering. If any Beta Region becomes generally available, your access to and use of Service Offerings in the generally available AWS region will be subject to the terms and conditions applicable to that AWS region. AWS does not guarantee that any Beta Service or Service Offering in any Beta Region will ever be made generally available, or that any generally available version will contain the same or similar functionality as the version made available by AWS during the term of the Beta Service or Beta Region, as applicable. AWS does not guarantee that any Beta Region will become generally available.

1.10.8. Beta Materials, Test Observations, Suggestions concerning a Beta Service or Beta Region, or any other information about or involving (including the existence of) any Beta Service or Beta Region are considered AWS Confidential Information. You will not disclose (including, but not limited to, in a press release or public statement) any Beta Materials, Test Observations, Suggestions concerning a Beta Service, or any other information about or involving (including the existence of) any Beta Service, except as agreed by AWS in writing.

1.10.9. ADDITIONAL WARRANTY DISCLAIMERS. WITHOUT LIMITING ANY DISCLAIMERS IN THE AGREEMENT OR THE SERVICE TERMS, THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS ARE NOT READY FOR GENERAL COMMERCIAL RELEASE AND MAY CONTAIN BUGS, ERRORS, DEFECTS OR HARMFUL COMPONENTS. ACCORDINGLY, AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT OR THESE SERVICES TERMS, AWS IS PROVIDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS AND BETA MATERIALS TO YOU "AS IS." AWS AND ITS AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS, INCLUDING ANY WARRANTY THAT THE BETA SERVICES, SERVICE

OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS AND ITS AFFILIATES AND 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. AWS' AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY FOR ANY BETA SERVICES WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE BETA SERVICES THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

1.10.10. Because the Beta Services and Materials involve features, technologies and services that are not yet generally available, you acknowledge that any violation of this Section 1.10 could cause irreparable harm to AWS for which monetary damages may be difficult to ascertain or an inadequate remedy. You therefore agree that AWS will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Section 1.10.

2. Amazon CloudFront

2.1. You must own or have all necessary rights to use any domain name or SSL certificate that you use in conjunction with Amazon CloudFront. You are solely responsible for the renewal, security and proper configuration of any SSL certificates that you provide for use with Amazon CloudFront, including any disclosure of your SSL certificates to third parties.

2.2. Amazon CloudFront requires you to store the original version of Your Content in an origin server (such as Amazon S3). If you use other Services to store the original version of Your Content, you are responsible for the separate fees you accrue for the other Services and for Amazon CloudFront.

2.3. While you will only be charged fees specified for the selected Price Class, Your Content you select for delivery from edge locations in a Price Class may from time to time be served from edge locations located outside the regions in that Price Class.

2.4. Amazon CloudFront's Geo Restriction feature may utilize a third party geo-location database, which may not be accurate in all situations.

3. Amazon Simple Queue Service (Amazon SQS)

3.1. You may not knowingly create and maintain inactive queues. We may delete, without liability of any kind, any of Your Content that sits in an Amazon SQS queue or any Amazon SQS queue that remains inactive for more than the number of days specified in the user documentation.

4. Amazon Elastic Compute Cloud

4.1. In connection with your use of Amazon Elastic Compute Cloud (including all instances and instance types, hosts and other resources, dedicated, reserved or on-demand, collectively “Amazon EC2”) and the Services, you are responsible for maintaining licenses and adhering to the license terms of any software you run.

4.2. Using Microsoft Software. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the “Microsoft Software”). If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, “High Risk Use”). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- Microsoft is an intended third-party beneficiary of this Section 4.2, with the right to enforce its provisions.

4.3. Using Novell Software. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Novell, Inc. or its licensors (collectively, the “Novell Software”). If you choose to use the Novell Software, Novell and its licensors require that you agree to these additional terms and conditions:

- Your use of the Novell Software is subject to the terms and conditions of the Novell End User License Agreement (“Novell EULA”) provided with the Novell Software. By using the Novell Software, you hereby agree to be bound by the terms of the applicable Novell EULA, which is presented the first time you access the relevant machine image.

4.4. Using Red Hat Software. In conjunction with the Services, you may be allowed to use certain software (including related support, maintenance, and documentation) developed, owned or provided by Red Hat, Inc. or its licensors (collectively, the “Red Hat Software”). If you choose to use the Red Hat Software, Red Hat and its licensors require that you agree to these additional terms and conditions:

- Red Hat disclaims any (i) warranties with respect to the Red Hat Software and (ii) liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from your use of the Red Hat Software.
- Your use of the Red Hat Software is subject to the terms and conditions of the Red Hat Cloud Software Subscription Agreement currently located at www.redhat.com/licenses/cloud_cssa/ (the “Red Hat CSSA”). By using the Red Hat Software, you hereby agree to be bound by the terms of the Red Hat CSSA.

4.5. Spot Instance Pricing. You may request that certain Amazon EC2 instances run pursuant to the Spot instance pricing and payment terms (“Spot Instance Pricing”) set forth on the Amazon EC2 product detail page on the AWS Site (each requested instance, a “Spot Instance”). You must request Spot Instances through the AWS Management Console or by using API tools (“Spot Instance Request”). As part of your Spot Instance Request, you must specify the maximum hourly price you are willing to pay to run the requested Spot Instances (“Your Maximum Price”). Unless you specify a permissible alternative termination date, your Spot Instance Request will remain active until we fulfill it or you cancel it. We set the price for Spot Instances (the “Spot Price”), which may vary over time based on a number of factors, including the amount of available compute capacity we have available and the price you and other customers are willing to pay for Spot Instances (e.g., supply and demand). While a requested Spot Instance remains running, you will be charged the current Spot Price in effect at the beginning of each instance hour. You will not be charged more than Your Maximum Price. We may terminate Spot Instances at any time and without any notice to you if we determine the current Spot Price equals or exceeds Your Maximum Price or for AWS capacity requirements. If we terminate your Spot Instance, you will only be charged for each full hour the Spot Instance ran. AWS may allow you to purchase Spot Instances of a fixed duration (each, a “Spot Block”), where the Spot Price for that Spot Instance (the “Block Price”) will remain constant for the duration of the Spot Block, and you will be charged the Block Price for the duration of your Spot Block. Spot Instances purchased as Spot Blocks run independently of the Spot Price, and will not be terminated because the Spot Price equals or exceeds Your Maximum Price. Spot Instances purchased as Spot Blocks may still be terminated for AWS capacity requirements and will terminate at the conclusion of the fixed duration. If a Spot Instance purchased as a Spot Block is terminated due to AWS capacity requirements, you will not be charged for that Spot

Instance. Unless you designate your Spot Instance Request as a persistent request, terminated Spot Instances will not automatically restart. You should save your work frequently and test your application to ensure it is fault tolerant and will correctly handle interruptions. We have no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from our termination of any Spot Instance. Spot Instances may not be used with certain Services, features and third-party software we specify, including Amazon DevPay, IBM software packages, or Microsoft SQL Server. You may not, directly, indirectly, alone or in cooperation with any third party, attempt to control, influence or manipulate the price for Spot Instances. Without limiting the foregoing, you may not submit requests for Spot Instances through any third party (e.g., “proxy bidding”) or share information with any third party regarding the maximum prices specified in your Spot Instance Requests. We may modify or terminate the Spot Instance Pricing program at any time. In addition to the Spot Instance Pricing, Spot Instances are subject to all data transfer and other usage fees applicable under the Agreement.

4.6. EC2 Reserved Instance Pricing. You may designate Amazon EC2 instances as subject to the reserved pricing and payment terms (“EC2 Reserved Instance Pricing”) set forth on the Amazon EC2 detail page on the AWS Site (each designated instance, a “EC2 Reserved Instance”). Scheduled EC2 Reserved Instances (“Scheduled Instances”) will terminate upon completion of the scheduled reservation. You may designate instances as EC2 Reserved Instances by calling to the Purchasing API or selecting the EC2 Reserved Instance option in the AWS console. When you designate instances as Reserved Instances, you must designate an availability zone, instance type, EC2 Reserved Instance type, and quantity for the applicable EC2 Reserved Instances. The EC2 Reserved Instances may only be used in the designated availability zone. We may change EC2 Reserved Instance Pricing at any time but price changes will not apply to previously designated EC2 Reserved Instances, except as described in this Section 4.6. If Microsoft increases the license fees it charges for Windows, or if Red Hat increases the license fees it charges for Red Hat Enterprise Linux (“RHEL”), we may make a corresponding increase to the per-hour usage rate (or institute a corresponding per-hour usage rate) for EC2 Reserved Instances with Windows or RHEL. Any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with Windows will be made between December 1 and January 31, and we will provide 30 days’ notice. For any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with RHEL we will provide 30 days’ notice. If this happens, you may: (a) continue to use your EC2 Reserved Instances with Windows or RHEL with the new per-hour usage price; (b) convert your EC2 Reserved Instances with Windows or RHEL to comparable EC2 Reserved Instances with Linux; or (c) terminate your EC2 Reserved Instances with Windows or RHEL and receive a pro rata refund of the up-front fee you paid for the terminated EC2 Reserved Instances with Windows or RHEL. We may terminate the EC2 Reserved Instance Pricing program at any time. EC2 Reserved Instances are nontransferable, except in accordance with the requirements of the RI Marketplace, but Scheduled Instances are not eligible for the RI Marketplace. EC2 Reserved Instances are noncancellable and you will owe the EC2 Reserved Instance Pricing for the duration of the term you selected, even if the Agreement is terminated.

All amounts paid in connection with the EC2 Reserved Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Reserved Instance type, or terminate the EC2 Reserved Instance Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated EC2 Reserved Instances. You may not purchase EC2 Reserved Instances for the purpose of reselling them in the RI Marketplace, and we reserve the right to refuse or cancel your purchase if we suspect you are doing so. Upon expiration or termination of the term of EC2 Reserved Instances, the EC2 Reserved Instance pricing will expire and standard on-demand usage prices will apply to the instances. In addition to being subject to EC2 Reserved Instance Pricing, EC2 Reserved Instances are subject to all data transfer and other fees applicable under the Agreement.

4.7 EC2 Reserved Instance (RI) Marketplace.

4.7.1. Eligibility. The rights to an active EC2 Reserved Instance can be offered for sale through the RI Marketplace as long as (1) the remaining term on the Reserved Instance is greater than one month, and (2) your payment of the upfront charge for it has been received and processed (for credit card purchases, 30 days after you have paid the upfront fee, and for invoice purchases, after you have paid the applicable invoice) (a “Marketable EC2 Reserved Instance”). The characteristics of the Marketable EC2 Reserved Instance (e.g., Instance Type, Platform, Region, Availability Zone, Tenancy, Hypervisor, Reserved Instance Type, Duration, and Hourly Price) will remain as originally designated. The term for the Marketable EC2 Reserved Instance will be the remainder of the original EC2 Reserved Instance term rounded down to the nearest month (for example, an EC2 Reserved Instance with 9 months and 16 days until expiration will be listed and sold as a 9 month Marketable EC2 Reserved Instance). You can be a “Seller” if you are a current AWS customer in good standing, you have a Marketable EC2 Reserved Instance associated with your AWS account, and you complete the registration process through your AWS account. Non-U.S.-based entities may not be Sellers without providing the Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) to establish that you are not a U.S. person. You can be a “Buyer” if you are a current AWS customer in good standing. You can resell an EC2 Reserved Instance that you previously purchased through the RI Marketplace. You may not resell an EC2 Reserved Instance that you purchased through a discount program (Reserved Instance Volume Discounts or otherwise) without obtaining our prior approval.

4.7.2. Submitting Marketable EC2 Reserved Instance for Sale. As a Seller, you will set the one-time price for your Marketable EC2 Reserved Instance. The hourly price will be the then-current hourly price for that type of EC2 Reserved Instance, and you will not receive any funds collected from payments associated with the hourly prices. You will pay the then-current fee to us specified on the AWS Site when your Marketable EC2 Reserved Instance is sold. Your Marketable EC2 Reserved Instance will be available for sale after you list it in the RI Marketplace, but it will remain yours and you will be able to use it until it is sold. You may remove a listing of Marketable EC2 Reserved Instance from the RI Marketplace at any time before it has been purchased by a Buyer. We may remove Marketable EC2 Reserved Instance from the RI Marketplace at any time for any

reason. Once sold and transferred to a Buyer, a Seller will have no rights to that Marketable EC2 Reserved Instance.

4.7.3. Our Role. As a Seller, you will be the seller of record of your rights to a Marketable EC2 Reserved Instance. Except as expressly set forth in these Service Terms, we are not involved in any underlying transaction between you and any Buyer. We or our affiliates may also participate in the market as a Seller or a Buyer.

4.7.4. Processing of Transactions; Collection of Transaction Proceeds. On Seller's behalf, we will process all payments for Transactions and collect the applicable Transaction Proceeds. "Transaction" means any sale of Marketable EC2 Reserved Instance through the RI Marketplace. "Transaction Proceeds" means the gross sales proceeds received by us from any Transaction. You will ensure that all fees and charges payable by Buyers for Marketable EC2 Reserved Instance are billed and collected through us and you will not offer or establish any alternative means of payment. We may impose transaction limits on some or all Buyers and Sellers relating to the value of any Transaction or disbursement, the cumulative value of all Transactions or disbursements during a period of time, or the number of Transactions that we will process over a period of time. We may withhold for investigation, or refuse to process, any of your Transactions that we suspect is fraudulent, unlawful or otherwise violates the terms of these Service Terms, the Agreement, or our Acceptable Use Policy. For each Transaction, we will not remit Transaction Proceeds to a Seller, and the Marketable EC2 Reserved Instance will be available to the Buyer, until after we have successfully processed payments for that Transaction from the Buyer.

4.7.5. Remittance of Transaction Proceeds to Sellers. At the end of each business day, we will pay to you all due and payable Transaction Proceeds that we have collected as of the date that is 2 business days prior to the date of payment. We will deduct from each payment any applicable fees and charges due to us related to Marketable EC2 Reserved Instances. The applicable fees and charges are posted on the AWS Site and may be changed from time to time. We may withhold, deduct, or setoff any amounts payable by you to us or our affiliates against any Transaction Proceeds. Payments will be made only to an ACH-enabled bank account located in the United States that you register with us. If there is an error in the processing of any Transaction, you authorize us to initiate debit or credit entries to your designated bank account, to correct such error, provided that any such correction is made in accordance with applicable laws and regulations. If we are unable to debit your designated bank account for any reason, you authorize us to resubmit the debit, plus any applicable fees, to any other bank account or payment instrument that you have on file with us or to deduct the debit and applicable fees from future Transaction Proceeds.

4.7.6. Taxes. Sellers are responsible for the calculation, validation and payment of any and all sales, use, excise, import, export, value added, withholding and other taxes and duties assessed, incurred or required to be collected ("Taxes") or paid for any reason in connection with any Transaction and with Marketable EC2 Reserved Instance. We are not obliged to determine whether any Taxes apply to any Transaction, and we are not responsible for remitting Taxes to any taxing authority with respect to any Transaction, or for reporting any information (including the payment of Taxes) with respect to any

Transaction. Each Seller will indemnify us and our affiliates against any claim or demand for payment of any Taxes imposed in connection with any Transaction, and for any fines, penalties, or similar charges imposed as a result of the Seller's failure to collect, remit or report any Taxes in connection with any Transaction.

4.7.7. Data Collection and Sharing. For each Seller, we will collect the necessary data and tax forms to enable compliance with applicable tax laws. For example, for U.S.-based Sellers, we will collect and retain Seller name and address, and may collect the tax identification number and other data as needed to comply with Form 1099K reporting requirements; for non-U.S.-based Sellers, we will collect and retain a Form W-8BEN tax form (which includes name, address, and a signature) as proof that you are exempt from Form 1099K reporting. For each Buyer, we will collect and retain the Buyer's name and address. Buyers and Sellers will not know the name of the other party to the Transaction until the Transaction is completed. Upon completion of the Transaction, we will share the applicable Buyer's city, state, and zip with the Seller so that the Seller can calculate the appropriate tax (if any) to remit to the appropriate government entity. We will share the Seller's legal name on the Buyer's invoice. Buyers and Sellers may not use information about the Transaction or about the other party gained in connection with a Transaction ("Transaction Information") for any purpose that is not related to the Transaction. For example, you may not, directly or indirectly: (1) disclose any Transaction Information to any third party, except as necessary for you to perform your tax obligations or other obligations under these Service Terms and only if you ensure that every recipient uses the information only for that purpose and complies with these restrictions; (2) use any Transaction Information for any marketing or promotional purposes whatsoever; (3) use any Transaction Information in any way inconsistent with applicable law; (4) contact a party to influence them to make an alternative sale or purchase; (5) disparage us, our affiliates or any of their or our respective products; or (6) target communications of any kind on the basis of the intended recipient being an RI Marketplace Buyer or Seller.

4.8 You may only use the AWS Management Pack for System Center on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Management Pack for System Center is governed by the license agreement, located here: AWS Management Pack for System Center License Agreement <http://aws.amazon.com/windows/system-center/aws-mp-license>.

4.9 Dedicated Instances. You may request that certain Amazon EC2 instances run on physically isolated host hardware dedicated to a single customer account (each requested instance, a "Dedicated Instance"), using the process set forth on the Amazon EC2 Dedicated Instance detail page on the AWS Site.

4.10 Dedicated Hosts.

4.10.1 You may request that Amazon provide the Amazon EC2 service to you on host hardware physically dedicated to a single customer account (each, a "Dedicated Host"), using the process set forth on the AWS Site.

4.10.2 You may designate Amazon EC2 Dedicated Hosts as subject to the reservation pricing and payment terms (“EC2 Dedicated Host Reservation Pricing”) set forth on the Amazon EC2 detail page on the AWS Site (each such host associated with a reservation, an “EC2 Dedicated Host Reservation”). You may associate EC2 Dedicated Host Reservations to Dedicated Hosts by calling APIs or using the EC2 Dedicated Host Reservation console. The EC2 Dedicated Host and associated EC2 Dedicated Host Reservation may only be used in the designated availability zone. We may change EC2 Dedicated Host Reservation Pricing at any time but price changes will not apply to previously designated EC2 Dedicated Host Reservations, except as described in this Section 4.10.2. We may terminate the EC2 Dedicated Host Reservation Pricing program at any time. EC2 Dedicated Host Reservations are nontransferable. EC2 Dedicated Host Reservations are noncancellable and you will owe the EC2 Dedicated Host Reservation Pricing for the duration of the term you selected, even if the Agreement is terminated. Dedicated Hosts associated to an active EC2 Dedicated Host Reservation cannot be unallocated from your account, and you will continue to pay for the Dedicated Host while still associated with the EC2 Dedicated Host Reservation. All amounts paid in connection with the EC2 Dedicated Host Reservations are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Dedicated Host type, or terminate the EC2 Dedicated Host Reservation Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated EC2 Dedicated Host Reservation. Upon expiration or termination of the term of an EC2 Dedicated Host Reservation, the EC2 Dedicated Host Reservation Pricing will expire and standard on-demand Dedicated Host prices will apply to the Dedicated Host. In addition to being subject to EC2 Dedicated Host Reservation Pricing, EC2 Dedicated Host Reservations are subject to all data transfer and other fees applicable under the Agreement.

4.11 Microsoft BYOL Licensing. Under this option, Amazon EC2 enables you to provision Amazon EC2 instances using your Microsoft Software and Microsoft Licenses (the “BYOL Program”). Unless otherwise specified in your agreement(s) with Microsoft, you can use this benefit only if you comply with the requirements [here](#) , and you (a) use Dedicated Instances or Dedicated Hosts; (b) launch from Virtual Machines (VMs) sourced from software binaries provided by you; and (c) run the instances within your designated AWS regions.

You must be eligible to use the BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using the Microsoft Software under the BYOL Program, you agree to the Microsoft EULA.

You agree that you have determined that your use of the BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted.

4.12 As part of using Amazon EC2, you agree that your Amazon EC2 resources may be terminated or replaced due to failure, retirement or other AWS requirement(s). We have

no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from the foregoing. THE USE OF AMAZON EC2 DOES NOT GRANT YOU, AND YOU HEREBY WAIVE, ANY RIGHT OF PHYSICAL ACCESS TO, OR PHYSICAL POSSESSION OF, ANY AWS SERVERS, EQUIPMENT, REAL OR PERSONAL PROPERTY, OR OTHER ASSETS.

5. Alexa® Web Services

5.1. You may use Alexa® Web Services to create or enhance applications or websites, to create search websites or search services, to retrieve information about websites, and to research or analyze data about the traffic and structure of the web.

5.2. You may not display data you receive via the Alexa® Services that has been cached for more than 24 hours.

5.3. You may not resell or redistribute the Alexa® Web Services or data you access via the Alexa® Web Services.

5.4. You may use data you receive from the Alexa® Web Services, such as web site traffic data, to enhance your application or website, but may not use it in any application whose primary purpose is to display the same or related data or whose primary purpose is to compete with www.alexacom .

6. Amazon Flexible Payments Service (Amazon FPS)

6.1. The terms in this Section 6 apply only to Amazon FPS and use of Your Content with the web-based payment service provided by Amazon Payments, Inc. (“Amazon Payments”) that enables the processing of payment transactions initiated by third parties, and that may include, without limitation, the processing and settlement of credit card transactions, bank transfers, or the administration of prepaid or post-paid balances (the “Payment Service”).

6.2. You may:

- access and use Amazon FPS to enable use of the Payment Service by users who have an appropriate Payment Service account (each, an “Amazon Payments User”) via Your Content in accordance with any applicable FPS Specifications (as defined below);
- install, copy, and use the software development kit provided by us as part of Amazon FPS, including the related development guides and technical documentation (collectively, the “FPS SDK”), and access and use the online testing environment made available by us (the “FPS Sandbox”), in each case as necessary to internally develop and test Your Content for use with the Payment Service; and
- create, incorporate, compile, and copy derivative works of the sample computer programming code provided by us for development and testing of Your Content (the “FPS Sample Code”) as part of Your Content for distribution in machine readable binary form or object code form to Amazon Payments Users as necessary for them to

use the Payment Service. Use of FPS Sample Code is also subject to any additional license terms included with the FPS Sample Code. Such additional terms will control in the event of any inconsistency or conflict with the Agreement.

6.3. The FPS SDK, FPS Sample Code, and FPS Specifications (as defined below) constitute Amazon Properties. Except as expressly authorized by this Section 6, you may not sublicense, loan, sell, assign, lease, rent, transfer, act as a service bureau, distribute or grant rights to any person or entity in Amazon FPS, the FPS SDK, the FPS Sandbox or the Payment Services.

6.4. You and Your Content will comply with any technical and operational specifications and other documentation or policies provided or made available by us or Amazon Payments with respect to Amazon FPS or the Payment Service respectively (the “FPS Specifications”). We reserve the right to update or modify the FPS Specifications at any time. Prior to making Your Content generally available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FPS, including without limitation that it complies with the FPS Specifications.

6.5. We may review and test Your Content to confirm that it operates properly with Amazon FPS and complies with the FPS Specifications, using review and test processes determined in our sole discretion. You agree to correct any material errors, defects or other non-compliance of which you become aware, including from review and test results provided by us. We may make modifications, updates or upgrades to Amazon FPS, the FPS SDK, or FPS Specifications. In such event, you will test and, if necessary, modify Your Content to ensure that it continues to operate properly with the then-current version of Amazon FPS, the FPS SDK, and FPS Specifications.

6.6. You must establish and maintain a payments account with Amazon Payments to use Your Content commercially with Amazon FPS and to access the Payment Service. Your use of the Payment Service is subject to Amazon Payment’s policies, procedures, and user agreements, and any breach of the foregoing will constitute a breach of the Agreement. In addition to the limitations described in the Agreement, any use of the Amazon Payments logo and trademark is subject to the trademark usage guidelines issued by Amazon Payments.

6.7. You are responsible for (a) the collection and payment of any and all sales, use, excise, import, export, value added and other taxes and duties assessed, incurred or required to be collected or paid for any reason in connection with any offer or sale of products or services by you, including Your Content, and (b) any payment transaction that is initiated using Your Content that is charged back or reversed (a “Chargeback”) to the extent that such Chargeback is attributable to any error, act or omission of you or Your Content and is not otherwise recovered by Amazon Payments from an Amazon Payments User. You will indemnify and reimburse Amazon Payments and its affiliates against any claim or demand for payment of any such taxes or any Chargebacks.

6.8. You represent, warrant, and covenant that you will at all times:

- represent the capabilities and features of the Payment Service consistent with our description of such capabilities and features and avoid false, deceptive, misleading or

unethical practices that may be detrimental to us or Amazon Payments, the Payment Service, Amazon Payments Users or other third parties;

- refrain from providing warranties or disclaimers with respect to the Payment Service;
- promptly investigate and report to us all complaints received by you with regard to Amazon FPS and the Payment Service, and make every reasonable effort to maintain and promote good public relations for us in the handling of any such complaints; and
- ensure that the terms of any agreements between you and any Amazon Payments User are consistent with the terms of the Agreement and these Service Terms.

7. Amazon DevPay Service (Amazon DevPay)

7.1. You may use Amazon DevPay to: (a) sell to end users (“Customers”) use of Your Content that you develop and make available with the Services (the “Bundled Application”), including machine images that you develop; (b) establish accounts for Customers that use the Bundled Application (“Customer Accounts”); (c) manage features of Customer Accounts; and (d) receive payments from Customers for Bundled Applications.

7.2. You will establish the pricing applicable to Customers for their use of any Bundled Application. We will only be responsible for collecting those fees that are fully disclosed and properly configured within the DevPay Service. The fees you charge to Customers for your Bundled Applications through the DevPay Service (as further described in Section 7.6 below) must constitute the full and complete fees you charge Customers for such Bundled Applications. You may not charge or impose any additional or supplemental fees for Bundled Applications other than those disclosed through the DevPay Service. While you are using the DevPay Service, you shall not establish any alternative means of payment for such Bundled Applications. The foregoing does not limit your ability to charge and receive payments for goods and services other than the Bundled Application sold through the DevPay Service.

7.3. You are responsible for designating all terms and conditions applicable to the use of the Bundled Application; provided that, use of the underlying Services are subject to the terms of the Agreement which will control in the event of a conflict. We may require users to register an AWS account (including agreeing to the terms of the Agreement) in order to use Amazon EC2 or other Services associated with the Bundled Application. You may not extend on behalf of us any written or oral warranty or guarantee, or make any representation or claim, with respect to the Services without our prior written consent. Upon termination of the Agreement or the [Amazon Payments, Inc. Customer Agreement](#) for any reason, all access by Customers with respect to your Bundled Applications may be terminated by us.

7.4. Except as set forth in Section 7.5 below, you are fully liable for all charges incurred for Services under your account identifiers or those assigned to your Customers for your Bundled Applications. All Services will be charged at the then current price applicable to such Services under the Agreement. Payments will be processed by Amazon

Payments, Inc. and are subject to the terms of the [Amazon Payments, Inc. Customer Agreement](#) , including your liability for chargebacks. All payments collected using the DevPay Service are subject to the then current processing fee described on the DevPay detail page on the AWS Site. Amounts owed under the Agreement may be deducted from proceeds collected under the [Amazon Payments, Inc. Customer Agreement](#) .

7.5. If we are unable to collect the fees you specify from your Customers for the sale of your Bundled Applications (“Customer Fees”) or a prior transaction for those fees is reversed, you will not be responsible for paying the fees for the Services used by you and your Customer (“Service Fees”) and AWS will have no obligation to remit or otherwise seek collection of the Customer Fees, provided that the payment failure is due to:

- AWS’s inability to charge a Customer’s credit card for the Customer Fees, or
- A transaction is reversed as a result of a Chargeback (as described in the [Amazon Payments, Inc. Customer Agreement](#)) because the transaction was not authorized or was otherwise fraudulent.

In addition, in the applicable month, the Customer Fees charged must exceed the Service Fees. In the event of such a payment failure, we may recover or otherwise set off any Customer Fees from you that we collected in the month to the extent they do not exceed the Service Fees. In the event that either you or AWS is subsequently able to collect the Customer Fees, you will pay to AWS the corresponding Service Fees as provided in the Agreement.

7.6. We will host and make available to Customers a customer interface (“Customer UI”) permitting (a) the display to Customers of certain pricing, terms and conditions and other information you provide to us regarding your Bundled Applications (“Subscription Information”) and (b) Customers to engage in certain functions with respect to your Bundled Applications, such as account establishment, account termination, payment authorization and termination rights. We will define and control the fields and format for the Customer UI and for Subscription Information. We retain all rights to the Customer UI, including its look and feel, and you will not copy or mimic the Customer UI in any manner.

7.7. You are responsible for ensuring and shall ensure that all Subscription Information (as you provide it to us and as it is ultimately shown on the Customer UI) is: (a) full, accurate and complete, (b) not misleading; and (c) in compliance, in all respects, with applicable laws. You must promptly update the Subscription Information when and as necessary to ensure that the Subscription Information continues to comply with the foregoing requirements, even if the updates are necessary as a result of changes we make to the data input fields or to the Customer UI.

7.8. You are responsible for providing customer service (if any) to Customers for your Bundled Applications. We shall have no obligation to provide customer or technical support to any Customer for Bundled Applications; provided that, we will provide support to Customers regarding billing and payment questions.

7.9. You will use the communication methods we establish through the DevPay Services for the administration of Customer Accounts, including, but not limited to, any communications regarding Customer Account termination or pricing changes.

7.10. You acknowledge and agree that we may take any of the corrective action regarding Customer Accounts to the extent we deem necessary or appropriate, in our sole discretion, to (a) comply with law, (b) enforce or apply the Agreement, the [Amazon Payments, Inc. Customer Agreement](#), or other agreements or policies applicable to the Services or DevPay Service, or (3) protect the rights, property or safety of our business, a Customer, or any third party. Corrective action may include (i) suspending, canceling or closing of Customer Accounts; (ii) re-establishment of Customer Accounts; and (iii) waiving or refunding of fees on Customer Accounts. We shall have no liability to you for taking any such actions. You shall promptly comply with any actions we take or may require of you regarding Customer Accounts. These actions may include, without limitation, reimbursing us for Customer refunds we issue, discontinuing provision of services on Customer Accounts we cancel, and re-establishment of services on Customer Accounts we re-establish. Should you ask us to close a Customer Account by using a method we have provided for that purpose, we will endeavor to close the Customer Account reasonably promptly, but we shall have no liability to you for the speed with which we do so or for our failure to do so. You shall indemnify and hold us and our employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys fees), arising out of or in connection with any claim based on or related to any actions we may take with respect to any Customer Account at your direction, including, without limitation, any closure of a Customer Account.

7.11. You acknowledge and agree that: (a) you have no expectation and have received no assurances that your business relationship with us will continue beyond the Term (or its earlier termination), that any investment by you in the promotion of any Bundled Application will be recovered or recouped, or that you will obtain any anticipated amount of profits; and (b) you will not have or acquire by virtue of the DevPay Services or otherwise any vested, proprietary or other right in the promotion of any Services or in any related goodwill created by your efforts.

8. Amazon SimpleDB Service (Amazon SimpleDB)

8.1. If during the previous six (6) months you have incurred no fees for Amazon SimpleDB and have registered no usage of Your Content stored in Amazon SimpleDB, we may delete, without liability of any kind, Your Content that is stored in Simple DB upon thirty (30) days prior notice to you.

9. Amazon Fulfillment Web Service (Amazon FWS)

9.1. You may only access and use Amazon FWS to query, access, transmit and receive product and shipping information related to your use of the Fulfillment by Amazon service ("FBA Service") sold and provided by Amazon Services LLC ("Amazon Services") in accordance with any applicable FBA Specifications (as defined below).

9.2. To use Amazon FWS, you must have an Amazon seller account (your “Seller Account”) that is in good standing and be registered to use the FBA Service. Your use of the FBA Service and your Seller Account is solely subject to Amazon Services’ policies, procedures, the Amazon Business Services Agreement or other applicable user agreements. Amazon FWS is only a technical interface that enables you to access and process certain information related to your Seller Account. AWS will have no liability to you or any third party related to your Seller Account.

9.3. You may use Amazon FWS only to administer product and shipping information associated with your Seller Account. When registering for Amazon FWS, you must use the same username and password which is associated with your Seller Account. You may not develop or use an application to access Amazon FWS that collects, processes or stores the account identifiers or other security credentials (including usernames and passwords) of any third party associated with AWS or any of its affiliates.

9.4. You and Your Content will comply with any technical and operational specifications, security protocols and other documentation or policies provided or made available by us with respect to Amazon FWS (the “FBA Specifications”). We reserve the right to update or modify the FBA Specifications at any time. Prior to making Your Content available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FWS, including, without limitation, that it complies with the FBA Specifications.

10. Amazon Elastic MapReduce

10.1. We may collect certain information about computing jobs you run using Amazon Elastic MapReduce, including CPU utilization, memory usage, IO performance, and error and information messages.

10.2. You are responsible for all fees incurred from your use of Amazon Elastic MapReduce regardless of the results obtained, the quality of the resulting data, or whether a computing job runs successfully. Use of Amazon Elastic MapReduce requires use of Amazon EC2 and Amazon S3, and certain features require use of Amazon SimpleDB. You are responsible for the separate fees you accrue for Amazon EC2, Amazon S3, and Amazon SimpleDB.

10.3. You are solely responsible for monitoring the status of your computing jobs. We may throttle or terminate computing jobs that we determine degrade the performance of Amazon Elastic MapReduce, the Services, or any component of the Services. We are not responsible for any data loss or data corruption that occurs as part of your computing jobs.

11. Amazon CloudWatch and Auto Scaling

11.1. You may only use Amazon CloudWatch to perform monitoring and auto-scaling functions in connection with Amazon EC2. Amazon CloudWatch enables Auto Scaling in connection with Amazon EC2. Auto Scaling requires use of both Amazon CloudWatch and Amazon EC2.

11.2. In connection with Auto Scaling, we may launch additional Amazon EC2 instances or terminate Amazon EC2 instances based on conditions you set. You are responsible for the separate fees you accrue for Amazon EC2. You are responsible for all fees incurred from your use of Amazon CloudWatch and Auto Scaling regardless of the results obtained or the quality or timeliness of the results. Charges for Amazon CloudWatch will accrue as soon as you use begin using Amazon CloudWatch or Auto Scaling functionality.

11.3. Amazon CloudWatch collects and stores certain information for the Amazon EC2 instances you are monitoring, including CPU utilization, data transfer, and disk usage and activity. Amazon CloudWatch metric data is kept for 14 days; we may delete CloudWatch metric data, without liability of any kind, at any time after 14 days.

12. Elastic Load Balancing

12.1. You may only use Elastic Load Balancing to provide load balancing functionality in connection with Amazon EC2. You must have instances running in all Availability Zones across which you want to balance loads with Elastic Load Balancing.

12.2. Use of Elastic Load Balancing requires use of Amazon EC2. You are responsible for the separate fees you accrue for Amazon EC2. You are responsible for all fees incurred from your use of Elastic Load Balancing regardless of the results obtained or the quality or timeliness of the results. Charges for Elastic Load Balancing will accrue as soon as you use begin using Elastic Load Balancing functionality.

13. AWS Import/Export

13.1. As part of AWS Import/Export Disk, you may send physical storage media (the “Media”) to us that we will use to either (a) transfer data contained on the Media into supported AWS Services as Your Content or (b) transfer certain of Your Content to the Media (such data contained on Media either before or after transfer, “Data”) and provide the Media to you.

13.2. You will not deliver to us, and we may refuse to accept any, damaged, defective or unreadable Media or any Media otherwise not shipped in accordance with the Agreement (collectively, “Unsuitable Media”). We may return or dispose of any Unsuitable Media, or erase Data on such Unsuitable Media. In addition, you will reimburse us for any expenses we incur in connection with any Unsuitable Media. If you request and we return Unsuitable Media to you, you agree that we will select the shipping carrier and handling standards for return of such Unsuitable Media in our sole discretion, and the carrier and standards may not be the same (and may cost more) than those we use for shipping media in connection with AWS Import/Export generally. For avoidance of doubt “Media” includes “Unsuitable Media”.

13.3. As part of AWS Import/Export Snowball, we will ship you an agreed upon number of network-attached storage appliances (each an “Appliance”) and provide you with access to the AWS Snowball Client (together with the software contained on the Appliance, and any updates or upgrades to the foregoing, the “Software”). AWS Import/Export Snowball availability is limited to certain AWS regions and account types;

please contact us to see if you qualify. You agree that you will not allow any Appliance to leave the United States state or non-U.S. country to which the Appliance is shipped until you deliver it (in the same U.S. state or non-U.S. country) to a carrier for redelivery to us. After you receive an Appliance, you may transfer certain of Your Content onto the Appliance as “Data” and provide the Appliance to the carrier for return to us. Once we receive the Appliance, we will transfer the Data on the Appliance into a supported AWS Service as Your Content.

13.4. You will comply with all specifications and documentation for AWS Import/Export as provided and updated by us from time to time, including shipping and encryption requirements, the [AWS Import/Export Disk Pack and Ship Check List](#), the AWS Import/Export Snowball User Guide, and any documentation on the AWS Site or an Appliance.

13.5. You will be solely responsible for all shipping and handling costs (which may include costs of freight and transit insurance) for shipping Media and Appliances to or from us. For AWS Import/Export Disk, we may pay some reasonable return shipping charges as described on the AWS Import/Export Disk section of the AWS Site. You are responsible for payment of all customs, duties, taxes and other charges in connection with Media and Appliances being shipped to or from us. Use of AWS Import/Export requires use of a supported AWS Service. You are responsible for the separate fees you accrue for AWS Services.

13.6. We have no liability or responsibility with respect to any delay, damage or loss incurred during shipment in connection with AWS Import/Export, including loss of Data. For AWS Import/Export Disk, you will bear the entire risk of loss of, or damage to, any Media (including Data) while in transit and you are solely responsible for obtaining insurance at your expense. For AWS Import/Export Snowball, you are responsible for the entire risk of loss of, or any damage to, an Appliance once it has been delivered by the carrier to your address until the carrier accepts the Appliance for delivery back to Amazon. If you have not provided an Appliance to the carrier for delivery to Amazon for any reason within 12 days of the date it was delivered to your address, we may charge you a late fee as described on the AWS Import/Export Snowball section of the AWS Site. If you have not provided an Appliance to the carrier for return to Amazon within 90 days of the date it was delivered to you, we may charge you a lost device fee of \$7500, in addition to the applicable late fees. If we receive an Appliance back from you and it has any damage which it did not have when we sent it to you, you may be charged the cost to us of fixing the damage or, if the damage cannot be reasonably fixed, the lost device fee described in the previous sentence.

13.7. You will retain title to any Media and Data we receive from you and store on an AWS Service as part of AWS Import/Export. You supply us with Media and Data entirely at your own risk. You should back-up Data prior to transfer onto an Appliance or Media and prior to delivery to us. Your Data should not include live or production data or any other data that you are not prepared to lose. We are not responsible for and will not be held liable for any damage to Media or any loss of Data. Our confirmed receipt of delivery does not: (a) indicate or imply that any Media, Appliance or Data has been delivered free of loss or damage, or that any loss or damage to any Media, Appliance or

Data later discovered occurred after confirmed receipt of delivery; (b) indicate or imply that we actually received the number of units of Media specified by you for such shipment; or (c) waive, limit or reduce any of our rights under the Agreement. We reserve the right to impose, and change, from time to time, volume limitations on the delivery of your Media, and you will comply with any of these restrictions or limitations.

13.8. You represent that you have all necessary rights to (a) provide the Media and Data to us for upload into supported AWS Services and (b) authorize our transfer of any Data specified by you to the Media. You represent that import or export of the Media or Data to or from us does not require a license under the laws or regulations of any country. We may reproduce Data as necessary to transfer it between Media or Appliances and supported AWS Services.

13.9. IN ADDITION TO THE DISCLAIMERS IN THE AGREEMENT, WE HEREBY DISCLAIM ANY DUTIES OF A BAILEE OR WAREHOUSEMAN, AND YOU HEREBY WAIVE ALL RIGHTS AND REMEDIES OF A BAILOR (WHETHER ARISING UNDER COMMON LAW OR STATUTE), RELATED TO OR ARISING OUT OF ANY POSSESSION, STORAGE OR SHIPMENT OF MEDIA OR DATA BY US OR OUR AFFILIATES OR ANY OF OUR OR THEIR CONTRACTORS OR AGENTS. YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA. You use the Appliances and Software entirely at your own risk. We are not responsible and will not be liable for any damage to, or any loss or misuse of, systems or equipment you use in connection with the Appliances and Software.

13.10. In addition to your indemnification obligations under the Agreement, you agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys' fees), arising out of or in connection with any claim arising out of (a) the Media (whether or not title has transferred to us) and Data, including any personal injury, death or property damage (including any damage caused by malicious or harmful code included in Data); (b) any sales, goods and services, use, excise, import, export, property, value added or other taxes or duties assessed or imposed on us or our affiliates in connection with or as a result of the storage, shipping or other actions taken by you with respect to the Appliances or taken by us with respect to the Media or Data; (c) any legal or regulatory violation, arising under the laws or regulations of any country, related to import or export of the Media or the Data.

13.11. Once AWS Import/Export services are complete, we will return the Media to you (for AWS Import/Export Disk) or delete the Data from the Appliance (for AWS Import/Export Snowball). We may return Media to you for any reason, including upon termination of the Agreement or the AWS Import/Export service. Returned Media will be sent to your designated shipping address. Media shipped to us for import into or export from supported AWS Services in the EU (Ireland) Region must originate from and be returned to an address within the European Union. If we have an outdated, incorrect or

prohibited address for you, we will attempt to notify you and you will have thirty (30) calendar days from the date we provide notification to supply a substitute address. If you do not supply a substitute address within thirty (30) calendar days of notification, the Media will be deemed Unsuitable Media subject to disposal. We may erase Data and dispose of Media in any manner and we have no obligation to reimburse or compensate you for any loss of Media or Data due to our disposal.

13.12. Notwithstanding anything to the contrary in the Agreement, you may give agents and subcontractors of your choosing access to the private key associated with your AWS account solely for the purpose of (a) preparing Data for import or export using AWS Import/Export or (b) confirming the integrity of Data imported or exported using AWS Import/Export. You remain fully responsible for and indemnify us for all activities undertaken by such third parties under your account. Other than as specifically set forth in this section, all terms and conditions of the Agreement continues to apply to your use of the Services.

13.13. The Appliances, the Software and all other proprietary information, know-how, programming, software, trademarks, trade secrets, plan drawings, requirements, specifications, designs, and patterns furnished or created by us or our agents or contractors and all property rights embodied therein are and will remain our sole property at all times. At no point do we sell, rent, lease or transfer any ownership or other rights to the Appliance to you. You may not use the Appliance in any manner not expressly permitted herein. Without limiting the foregoing, you will not, and will not permit or authorize third parties to (or attempt to), (a) disassemble or reverse engineer the Appliance or the Software; (b) open, modify, alter or otherwise tamper with the Appliance; (c) circumvent or disable any features or measures in the Appliance or the Software. Your use of the Software is governed by the licenses included with the Software. Certain components of the Software included on Appliances are governed by the open source software licenses identified [here](#) . Your license rights with respect to such components are defined by the applicable open source software license.

13.14. For AWS Import/Export, Disk, we will not act as the importer of record for your shipments of Media or Data. If we are importing or exporting your shipments of Media or Data into the Asia Pacific (Singapore) Region, you will not act as the importer of record and you represent and warrant that: (a) You are not a resident of Singapore; (b) You have a business establishment or fixed establishment outside of Singapore and not in Singapore; (c) You are domiciled outside Singapore if you have no business or fixed establishment in any country; (d) You are not registered or required to be registered for GST in Singapore.

You will notify us if, at any time, you are using the AWS Import/Export Disk service to ship Media or Data into the Asia Pacific (Singapore) Region and you are not acting as the importer of record, and you become unable to make any of the above representations and warranties.

If you are not acting as the importer of record on your shipment of Media or Data to the Asia Pacific (Singapore) Region, then the Media or Data must (i) be returned to a

location outside of Singapore, (ii) be exported on an FCA basis; and (iii) you must be importer of record in the country that the Media or Data is returned to.

14. Amazon Virtual Private Cloud (Amazon VPC)

14.1. You may only use Amazon VPC to connect your computing resources to certain AWS computing resources via a Virtual Private Network (VPN) connection.

14.2. Use of Amazon VPC requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with Amazon VPC. When you transfer data between AWS computing resources running inside Amazon VPC and AWS computing resources running outside Amazon VPC, you will be charged VPN data transfer rates in addition to any applicable Internet data transfer charges. VPN connection charges accrue during any time your VPN connection is in the “available” state.

14.3. You are solely responsible for the configuration, operation, performance and security of all equipment and computing resources you use with Amazon VPC, including any gateways or other devices you use to connect to Amazon VPC.

15. AWS Multi-Factor Authentication (AWS MFA)

15.1. You may only use AWS MFA in connection with accessing your AWS account.

15.2. Your use of AWS MFA requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with AWS MFA.

15.3. You are solely responsible for the procurement and for the configuration, operation, performance and security of any hardware or non-AWS software that you use in connection with AWS MFA, including any compatible authentication devices.

16. Amazon Relational Database Service (Amazon RDS)

16.1. You may only use Amazon RDS to store, query, retrieve and serve data and other content owned, licensed or lawfully obtained by you. You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for the proper configuration of database security groups and other security settings associated with Amazon RDS.

16.2. You may store snapshots of Your Amazon RDS Content for later use in Amazon RDS but snapshots cannot be downloaded outside the Services.

16.3. We may terminate your Amazon RDS database instance if you attempt to access or tamper with any software we pre-load on the database instance, including the operating system software running on the database instance.

16.4. You are responsible for configuring your backup retention period to give yourself enough time to recover data from your backups in the event of a hardware or file system failure.

16.5. Reserved DB Instance Pricing. You may designate Amazon RDS database instances as subject to the reserved pricing and payment terms (“Reserved DB Instance Pricing”) set forth on the Amazon RDS detail page on the AWS Site (each designated instance, a “Reserved DB Instance”). You may designate database instances as Reserved DB Instance by calling to the Purchasing API or selecting the Reserved DB Instance option in the AWS console. When you designate a database instance as a Reserved DB Instance, you must designate a region, instance type and quantity for the applicable Reserved DB Instances. The Reserved DB Instances may only be used in the designated region. We may change Reserved DB Instance Pricing at any time but price changes will not apply to previously designated Reserved DB Instances. We may terminate the Reserved DB Instance Pricing program at any time. Reserved DB Instances are noncancellable, and you will owe the Reserved DB Instance Pricing for the duration of the term you selected, even if the Agreement is terminated. Reserved DB Instances are nontransferable and all amounts paid in connection with the Reserved DB Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved DB Instance type, or terminate the Reserved DB Instance Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved DB Instances. Upon expiration or termination of the term of a Reserved DB Instance, the Reserved DB Instance Pricing will expire and standard on-demand usage prices will apply to the database instance. In addition to being subject to Reserved DB Instance Pricing, Reserved DB Instances are subject to all data transfer and other fees applicable under the Agreement.

16.6. Using Oracle Software.

16.6.1 “License Included”. As part of the Services, you may be allowed to use certain software (including related documentation) described on the AWS Site developed and owned by Oracle America, Inc. or its affiliates (“Oracle”) and Oracle’s licensors (collectively, the “Oracle Software”). If you choose to use the Oracle Software and do not already have a license from Oracle for that Oracle Software, Oracle and its licensors require that you agree to these additional terms and conditions:

- Oracle or its licensors retains all ownership and intellectual property rights in the Oracle Software, and title to the Oracle Software does not transfer to you or any third party by virtue of this Agreement.
- The Oracle Software is subject to a restricted license and may only be used in connection with the Service Offerings, and only by the individual or legal entity that entered into the Agreement.
- You may only use the Oracle Software for your internal business operations and in accordance with the Agreement. You may permit agents or contractors (including outsourcers) to use the Oracle Software on your behalf for the purposes set forth in, and subject to, the Agreement, provided you are responsible for the agent’s, contractor’s and outsourcer’s compliance with the Agreement in connection with such use.

- You may not:
 - assign, grant, or transfer the Oracle Software or any interest in the Oracle Software to another individual or entity, and if you purport to grant a security interest in the Oracle Software, the secured party will have no right to use or transfer the Oracle Software;
 - use the Oracle Software for rental, timesharing, subscription services, hosting, or outsourcing;
 - remove or modify any notice of Oracle's or its licensors' proprietary rights;
 - make the Oracle Software available in any manner to any third party for use in the third party's business operations;
 - duplicate, reverse engineer (unless required by law for interoperability), disassemble or decompile the Oracle Software (including by reviewing data structures or similar materials produced by the Oracle Software); or
 - publish any results of benchmark tests run on the Oracle Software.
- Third party technology that may be appropriate or necessary for use with some Oracle Software is specified in the related documentation, and that third party technology is licensed to you only for use with the Service Offerings and under the terms of the third party license agreement specified in the documentation, not this Agreement.
- To the extent permitted by applicable law, Oracle disclaims any liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from your use of the Oracle Software.
- Notwithstanding anything to the contrary elsewhere in the Agreement, Oracle is an intended third party beneficiary of the Agreement, but solely with respect to this Section 16.6.1 of these Service Terms.
- The Uniform Computer Information Transactions Act does not apply to your use of the Oracle Software.
- Upon any termination of the Agreement, you must discontinue use of the Oracle Software and any related documentation.

16.6.2 "Bring-Your-Own-License" (BYOL). Under the BYOL option, Amazon RDS enable you to provision Oracle Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the Oracle Software. You can use the Oracle Software with Amazon RDS if you meet the following conditions:

- You must have a valid license with "Software Update License & Support" for the Oracle Software you wish to run. The terms of your existing license and support agreement(s) with Oracle continue to apply to your use of the Oracle Software; and

- You must follow Oracle's current policies for licensing Oracle Database software in the cloud computing environment. The database instances using the Oracle Software with Amazon RDS reside in the Amazon EC2 environment.

16.7 Using Microsoft Software.

16.7.1 "License Included." In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the "Microsoft Software"). If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, "High Risk Use"). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- SQL Server Web Edition may be used only to support public and Internet accessible Web pages, Web sites, Web applications or Web services. It may not be used to support line of business applications (e.g., Customer Relationship Management, Enterprise Resource Management and other similar applications).

16.7.2 License Mobility with Software Assurance (Bring Your Own License or BYOL). Under this option, Amazon RDS enable you to provision Microsoft SQL Server

Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the SQL Server Software. You can use this benefit if only you meet the requirements and have signed up as described [here](#).

16.7.3 Microsoft is an intended third-party beneficiary of this Section 16.7, with the right to enforce its provisions.

17. Amazon Simple Notification Service (Amazon SNS)

17.1. You may only use Amazon SNS to send notifications to parties who have agreed to receive notifications from you.

17.2. We may throttle or restrict notifications if we determine, in our sole discretion, that your activity may be in violation of the AWS Acceptable Use Policy or the Agreement.

17.3. Your notifications sent through Amazon SNS may be blocked, delayed or prevented from being delivered by destination servers and other reasons outside of our control and there is no warranty that the service or content will be uninterrupted, secure or error free or that notifications will reach their intended destination during any stated time-frame. In addition, you acknowledge that we may not be able to provide the service if a wireless carrier delivering Amazon SNS notifications by short messaging service (SMS) terminates or suspends their service. Your payment obligations may continue regardless of whether delivery of your notifications are prevented, delayed or blocked.

17.4. You may not use Amazon SNS to send SMS messages that include Premium Content (as defined in the Mobile Marketing Association Guidelines). You may not charge recipients for receiving Amazon SNS notifications by SMS unless you have obtained the recipient's express consent. You must advise recipients receiving Amazon SNS notification by SMS that wireless carriers may charge the recipient to receive Amazon SNS notifications by SMS. You must obtain our prior written consent before using Amazon SNS to send SMS messages for:

- financial transactions or payment services (e.g., mobile banking, bill presentment, bill payment, money transfer, peer-to-peer payment or lending credit, debit or stored value payment services);
- charitable programs (e.g., soliciting donations for a non-profit organization);
- sweepstakes or contests;
- advertisements or promotions for commercial products, goods or services; or
- location-based services (e.g., where a recipient receives messages based on the geographical location of the recipient's wireless device).

17.5. Any third party push notification platform that you use in connection with Amazon SNS is Third Party Content under the Agreement, and features of Amazon SNS that depend on such platforms may not be secure, uninterrupted or error-free. Your use of such push notification platform is subject to the platform's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change,

discontinue or deprecate support for a push notification platform for any reason at any time.

17.6. You and any of your applications that use Amazon SNS must comply with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

17.7. Through your use of Amazon SNS you will not:

- Transmit any material that contains viruses, Trojan horses, worms or any other malicious, harmful, or deleterious programs.
- Offer or purport to offer any Emergency Services. “Emergency Services” means services that allow a user to connect with emergency services personnel or public safety answering points such as 911 or E911 services.
- Materially violate or facilitate the material violation of any local or foreign law, rule, regulation or order, including laws regarding the transmission of data or software
- Transmit material that is sexually explicit, relates to “adult services”, or contains sensitive financial or identifying information (such as social security numbers)
- Resell, sublicense or timeshare the Services or use them on behalf of anonymous or other third parties.
- Use the Services in hazardous environments (such as operation of nuclear facilities, aircraft navigation, or any other use that may result in foreseeable risk of injury, death, or destruction of property).

18. Consolidated Billing

18.1. You may only use Consolidated Billing as described in this Section and on the AWS Site to (i) link an AWS account (the “Paying Account”) with another AWS account (each, a “Linked Account”), or (ii) allow an AWS account to be linked to a Paying Account. You may only link accounts held by you, your affiliates or your employees, or by your agents or subcontractors currently doing work on your behalf. If an agent or subcontractor ceases doing work on your behalf, you will promptly unlink the applicable account. When accounts are linked, the Paying Account will be billed for and will pay all applicable charges for each Linked Account in accordance with the payment provisions in the Agreement while the accounts are linked. By linking your Linked Account to a Paying Account, you consent to disclosing your billing and account activity for that Linked Account to the Paying Account. We will determine the number of accounts that may be linked. An account may unlink another account from it at any time. As soon as a Linked Account is unlinked from a Paying Account, the Linked Account will be billed for and will pay all applicable charges for the Linked Account in accordance with payment provisions in the Agreement. If a Paying Account is terminated for failure to satisfy the payment provisions in the Agreement, then all linked Accounts associated with the Paying Account will be unlinked. We may unlink a Linked Account from a Paying

Account at any time upon notice to both accounts in accordance with the Agreement, except that accounts linked in violation of this Section 18.1 may be unlinked by us immediately and without notice. Paying Accounts and Linked Accounts are jointly and severally liable for all fees accrued by Linked Accounts while the accounts are linked. Accordingly, if a Paying Account fails to pay for fees accrued by a Linked Account while the accounts are linked, the Linked Account remains liable for such fees.

18.2. When you use the CreateLinkedAccount API to create an AWS account (each, a “Programmatically Created Account”), (i) each Programmatically Created Account is a Linked Account; (ii) the AWS account that you used to access the API is the Paying Account; (iii) except as otherwise provided in the Paying Account’s Agreement, each Programmatically Created Account is governed by the terms of the [AWS Customer Agreement](#); (iv) except as otherwise authorized by AWS, each Programmatically Created Account may be used only by you or your agents or contractors performing work on your behalf and may not be created for any third party; (v) only AWS may unlink a Programmatically Created Account from the Paying Account; and (vi) you are responsible for ensuring that users abide by the terms governing each Programmatically Created Account and for all activities that occur under such account.

19. AWS Identity and Access Management (IAM)

19.1. You may use IAM to create additional sets of security credentials (the “User Credentials”) under your AWS account, the format of which may include a username and password, roles, policies, permissions, access keys, and/or a security token. The User Credentials are subject to change: (a) by you through the IAM APIs, or (b) if we determine in our reasonable discretion that a change is necessary. We will promptly notify you of any change we make to the User Credentials.

19.2. You will ensure that all use of the Services under the User Credentials complies with the terms and conditions of the customer agreement between you and us that governs your use of the Services.

19.3. You are responsible for all applicable fees associated with use of the Services in connection with IAM, including fees incurred as a result of any User Credentials. You are responsible for maintaining the secrecy and security of the User Credentials (other than any key that we expressly permit you to use publicly). You are solely responsible, and we have no liability, for any activities that occur under the User Credentials, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of all User Credentials created under your AWS account, including credentials that you have used IAM to create or disclose to other parties.

19.4. Except as otherwise provided by AWS, you may only use User Credentials for your internal use and may not expose your User Credentials publicly. You may not sell, transfer or sublicense or authorize the creation of User Credentials (other than public use of any key that we expressly permit you to use publicly) to any other party; provided that, you may disclose or cause to be disclosed User Credentials to your agents or subcontractors that are performing services for you, solely to allow the agents or

subcontractors to use the Services on your behalf in accordance with the agreement between you and us that governs your use of the Services.

19.5. Any third party identity provider that you use in connection with the Service Offerings is Third Party Content under the Agreement and may be provided directly to you by a third party under separate terms and conditions. You are solely responsible for complying with those terms and conditions. We may change, discontinue or deprecate support for an identity provider for any reason, including if the continued use of the identity service (a) poses a security or intellectual property issue, (b) is economically or technically burdensome, or (c) must be terminated to comply with the law or requests of governmental entities.

20. Amazon Route 53

20.1. You may use Amazon Route 53 to answer Domain Name System (DNS) queries for your applications.

20.2. You will not create a hosted zone for a domain that you do not own or have authority over.

20.3. All DNS records (other than Private DNS records) used in connection with Amazon Route 53 will be publicly available and AWS will have no liability for disclosure of those DNS records.

20.4 Domain name registration services are provided under our [Domain Name Registration Agreement](#).

21. AWS Elastic Beanstalk

21.1. The URL used in connection with an AWS Elastic Beanstalk environment will have the formulation [myapp].elasticbeanstalk.com. You will select the “myapp” portion of the URL and will not:

- include any trademark of Amazon or its affiliates, or a variant or misspelling of a trademark of Amazon or its affiliates – for example, “endlessboots”, “amaozn”, “smallpartsstore”, “amazonauctions”, “kindlemagazines”, or “kindlewirelessreader” would be unsuitable; or
- otherwise violate the intellectual property rights of any third party or the AWS Acceptable Use Policy (including, without limitation, containing any offensive, harmful or illegal content).

AWS may reject any URL that fails to comply with this Section. Further, AWS may modify any URL in order to make it compliant with this Section. In addition, AWS may treat any URL that fails to comply with this Section as Prohibited Content.

21.2. The [myapp] portion of the URL is reserved for you only during the time your application environment is running. If you stop running your application environment at any time, for any reason, the [myapp] portion of the URL you were using to run the application environment will no longer be available to you, and will be returned to a pool from which it may be used by another AWS customer.

21.3. AWS may make available reference or sample applications for you to use in connection with AWS Elastic Beanstalk (“Elastic Beanstalk Sample Apps”). Elastic Beanstalk Sample Apps are provided “as is” and you will be charged the same fees for running Elastic Beanstalk Sample Apps as you would be charged for running your own application.

21.4. AWS Elastic Beanstalk is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS Elastic Beanstalk.

22. Amazon Simple Email Service (SES)

22.1. We take steps to increase the security and reliability of email you send, attempt to send, or receive using SES (“SES Email”). Like many email service providers, when you send, attempt to send, or receive an email, we (or our third-party providers) may store and scan your SES Email and Your Content included in SES Email. This helps us protect you and SES by preventing and blocking “spam” e-mails, viruses and spyware, and other harmful or unwanted items from being sent and received over SES.

22.2. Your use of SES and all SES Email must comply with the AWS Acceptable Use Policy and the Agreement. We may throttle, suspend or terminate your access to SES, or block or decline to send and/or receive any SES Email, if we determine in our sole discretion that

- our scan of SES Email or Your Content included in SES Email reveals abusive or low quality email (such as “spam”),
- SES Email bounces back to us or we receive abuse complaints (including complaints from third parties) in connection with your SES Email,
- the source or ReturnPath email address you have provided us for “address bounces” or complaints is not successfully receiving email, or
- your use of SES Email does not comply with the AWS Acceptable Use Policy or the Agreement, or
- your SES Emails or Your Content include an attachment in a format that we do not support.

22.3. Your SES Emails may be blocked, delayed or prevented from being delivered by destination email servers and other reasons outside of our control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed or blocked.

22.4. You are solely responsible for ensuring any emails you send and receive using SES comply with the Federal CAN-SPAM Act. AWS is not the “sender” as defined in the Federal CAN-SPAM Act. You will not use SES in connection with an open mail relay, including, without limitation, an open mail relay in the form of an SMTP server, unrestricted web form, or otherwise.

22.5. Your SES Emails may be blocked, delayed or prevented from being received due to your configuration of the Service. You are solely responsible for the proper configuration of the Service to ensure the receipt of emails.

23. AWS CloudFormation

23.1. You may use AWS CloudFormation to create a collection of AWS resources and provision them.

23.2. AWS may make sample templates available for you to use in connection with AWS CloudFormation. All sample templates are offered “as is” and you are solely responsible for your use of the sample templates.

23.3. Any templates you use in connection with AWS CloudFormation must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

23.4. AWS CloudFormation is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS CloudFormation.

24. AWS Direct Connect

24.1. You may use AWS Direct Connect to establish a dedicated network connection between your network and your AWS resources by using connection types and locations supported by AWS. When you establish a dedicated connection, your network traffic that would have otherwise been routed over the Internet may be routed through your dedicated network connection, including your network traffic sent to or from (i) services offered by other affiliates of Amazon.com, Inc. or (ii) the AWS resources of other AWS customers.

24.2. The hardware and equipment you use with AWS Direct Connect must comply with the Documentation provided by AWS. You are responsible for protecting your AWS Direct Connect connections, including using physical security, firewalls and other network security tools as appropriate.

24.3. AWS will permit data center operator or other service provider to connect your hardware to AWS’s hardware at the AWS Direct Connect location(s) that you select. AWS will provide the necessary information to enable the data center operator or other service provider to establish and monitor this connection, including your name, email address, network configuration, activity information, and AWS account number.

24.4. You are responsible for your separate relationship with the data center operator or other service provider, including compliance with your agreement with, and the policies and procedures of, the data center operator or other service provider, and payment of applicable fees to the data center operator or other service provider. You are responsible for providing or procuring (and AWS will not own) any equipment or cabling necessary to establish this dedicated connection. Neither AWS nor any of its affiliates are responsible for the actions, errors or omissions of any employees or contractors of

data center operators or service providers, including if the employees or contractors fail to follow instructions from you or AWS.

24.5. We may disconnect your AWS Direct Connect connection at any time for any reason. If the connection you establish as part of AWS Direct Connect is temporarily unavailable or terminated, AWS will route traffic bound for your AWS resources over the public Internet and AWS's standard data transfer charges will apply. However, if you are using Amazon Virtual Private Cloud (VPC), traffic bound for your Amazon VPC resources will be routed through an IPsec VPN connection. If an IPsec VPN connection is unavailable, traffic bound for your Amazon VPC resources will not be delivered.

25. Amazon ElastiCache

25.1. You may only use Amazon ElastiCache to store, query, retrieve and serve Your Content. You are solely responsible, for the proper configuration of all security settings associated with Amazon ElastiCache.

25.2. You may not access or tamper with any software we install on the cache nodes as part of Amazon ElastiCache.

25.3. Amazon ElastiCache is designed for the ephemeral storage of Your Content. You are responsible for maintaining a persistent data storage for Your Content, and routinely archiving Your Content to prevent the loss of Your Content.

25.4. Replacement cache nodes automatically generated by Amazon ElastiCache may have different IP address, and you are responsible for reviewing your application configuration to ensure that your cache nodes are associated with the appropriate IP addresses.

25.5. We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the cache nodes as part of Amazon ElastiCache.

25.6. Reserved Cache Node Pricing. You may designate Amazon ElastiCache cache node as subject to the reserved pricing and payment terms ("Reserved Cache Node Pricing") set forth on the Amazon ElastiCache detail page on the AWS Site (each designated instance, a "Reserved Cache Node"). You may designate cache nodes as Reserved Cache Nodes by calling to the Purchasing API or selecting the Reserved Cache Node option in the AWS console. When you designate a cache node as Reserved Cache Node, you must designate a region, cache node type, Reserved Cache Node type, and quantity for the applicable Reserved Cache Node. The Reserved Cache Node may only be used in the designated region. We may change Reserved Cache Node Pricing at any time but price changes will not apply to previously designated Reserved Cache Nodes. We may terminate the Reserved Cache Node Pricing program at any time. Reserved Cache Nodes are nontransferable and all amounts paid in connection with the Reserved Cache Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Cache Node type, or terminate the Reserved Cache Node Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any

previously designated Reserved Cache Nodes. Upon expiration or termination of the term of a Reserved Cache Node, the Reserved Cache Node Pricing will expire and standard on-demand usage prices will apply to the cache node. In addition to being subject to Reserved Cache Node Pricing, Reserved Cache Nodes are subject to all data transfer and other fees applicable under the Agreement.

26. AWS Support

26.1. We will provide “Support” in accordance with the terms of AWS Support Features page available at <http://aws.amazon.com/premiumsupport> (the “Guidelines”). AWS Support is available only as described in the Guidelines. If you are experiencing problems with one or more Services in connection with your use of any Content that was provided to you by a third party (someone other than yourself or AWS) then AWS Support is not available.

26.2. In providing AWS Support, AWS will use commercially reasonable efforts to (a) respond within the “Response Times” set forth in the Guidelines for all properly submitted cases from authorized individuals, and (b) work towards the identification and resolution of the problems submitted. When submitting a case, you may designate the severity level of a problem; provided that, we reserve the right to reclassify the severity level in our reasonable opinion. All Response Times are measured from the point when a case has been properly submitted by an authorized individual to us. Cases may be submitted as specified in the Guidelines. We do not represent, warrant or guarantee that (i) we will always be able to resolve a case fully, (ii) you will no longer experience a problem, (iii) we will provide a bug fix, patch or other workaround in connection with the identified problem, or (iv) any support or advice will result in any performance efficiency or improvement. You are solely responsible for the implementation and results of any suggestions or advice received.

26.3. Unless otherwise set forth in the Guidelines, AWS Support fees will be the greater of (a) the specified minimum monthly fee, or (b) a percentage of your monthly usage charges for all Services during the billing period. Regardless of when you sign up or terminate AWS Support, you are obligated to pay for a minimum of thirty (30) days of support each time you register to receive the service. Implementation of any suggested configurations or improvements may result in additional fees and charges. We reserve the right to refuse to provide AWS Support to any customer that frequently registers for and terminates the service.

27. AWS GovCloud (US) Service Terms

27.1 You are responsible for satisfying any applicable eligibility requirements for using the AWS GovCloud (US) Region including providing accurate and current registration information. We may require you to provide additional registration information before we permit you to access the AWS GovCloud (US) Region. Such information may include your U.S. person status, as defined by 22 CFR part 120.15 (“US Person”), and whether you are subject to export restrictions under U.S. export control laws and regulations. We may make, directly or through third parties, any inquiries we consider necessary to validate information that you provide to us, including without limitation checking

commercial and/or governmental databases. While we may take steps to verify the identity of our Customers, we cannot and do not guarantee any Customer's identity.

27.2 AWS is responsible for maintaining access controls to the AWS GovCloud (US) Region that limit AWS personnel's physical and logical access to the "AWS Network" to US Persons only. The AWS Network consists of AWS's internal data center facilities, servers, networking equipment, and host software systems that are within AWS's reasonable control and are used to provide the AWS Services. You are responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer or End User account access, data transmission, encryption, and appropriate storage and processing of your Content within the AWS GovCloud (US) region. AWS makes no representation or warranty related to the US Persons status of any Customer or End Users that may be granted access to the AWS GovCloud (US) Region by other Customers and their End Users.

27.3 You are responsible for verifying the adequacy of the AWS GovCloud (US) Region for the processing and storage of your Content and that your use of AWS Services will comply with the laws and regulations that may govern your Content. You are also solely responsible for verifying that End Users are eligible to access your Content in the AWS GovCloud (US) region.

27.4 You may only use Amazon VPC to connect your computing resources to the AWS GovCloud (US) region.

27.5 AWS Services may not be used to process or store classified data. If you or your end users introduce classified data into the AWS Network, you will be responsible for all sanitization costs incurred by AWS.

28. Amazon DynamoDB

28.1 You will be charged for the throughput capacity (reads and writes) you provision in your Amazon DynamoDB tables even if you do not fully utilize the provisioned capacity.

28.2 The actual reads and writes performance of your Amazon DynamoDB tables may vary and may be less than the throughput capacity that you provision.

28.3 Reserved Capacity Pricing. You may purchase reserved throughput capacity (reads and writes) subject to the pricing and payment terms set forth on the Amazon DynamoDB detail page on the AWS Site ("Amazon DynamoDB Reserved Capacity"). You may purchase Amazon DynamoDB Reserved Capacity by submitting a request through the AWS console. When you purchase Amazon DynamoDB Reserved Capacity, you must designate a region, quantity, and term. You will be charged (1) a one-time, up-front fee and (2) an hourly fee for each hour during the term based on the amount of Amazon DynamoDB Reserved Capacity you purchase. The Amazon DynamoDB Reserved Capacity may only be used in the designated region and only by the account that purchased the Amazon DynamoDB Reserved Capacity. We may change the pricing for Amazon DynamoDB Reserved Capacity at any time, but price changes will not apply to previously purchased Amazon DynamoDB Reserved Capacity. We may terminate the Amazon DynamoDB Reserved Capacity program at any time.

Amazon DynamoDB Reserved Capacity is nontransferable and all amounts paid in connection with the Amazon DynamoDB Reserved Capacity are nonrefundable, except that if we terminate the Agreement (other than for cause) or the Amazon DynamoDB Reserved Capacity program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously purchased Amazon DynamoDB Reserved Capacity. Upon expiration or termination of the term of any Amazon DynamoDB Reserved Capacity, standard on-demand usage prices will apply to the your use of Amazon DynamoDB. Amazon DynamoDB Reserved Capacity is also subject to all storage, data transfer and other fees applicable under the Agreement.

28.4 You may install the local version of DynamoDB only on computer equipment owned or controlled by you and may use it solely (a) for your internal business purposes and (b) in connection with the Services. Your use of DynamoDB Local is governed by the DynamoDB Local License Agreement, located here: [DynamoDB Local License Agreement](#).

29. AWS Storage Gateway

29.1 You may only use the AWS Storage Gateway on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Storage Gateway is governed by the AWS Storage Gateway License, located here: [AWS Storage Gateway License Agreement](#).

30. AWS Marketplace

30.1 The AWS Marketplace is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content of third parties offered through the AWS Marketplace constitutes “Third Party Content” under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

30.2 Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

30.3 AWS may stop providing the AWS Marketplace (or any features of or listings within the AWS Marketplace) to you at AWS’s sole discretion, without prior notice to you. In

addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

30.4 You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace. This may include one-time payments as well as recurring payments. A “recurring payment” is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g. annually or monthly). The applicable fees and billing periods for the Content are listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. You may cancel your subscriptions at any time by logging into “Your Software Subscriptions” on the AWS Site. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

31. AWS Data Pipeline

31.1 You may only use the AWS Data Pipeline on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services.

31.2 Your use of the AWS Data Pipeline Remote Runner is governed by the AWS Data Pipeline Remote Runner License, located here: [AWS Data Pipeline Remote Runner License Agreement](#).

32. Amazon Elastic Transcoder

32.1 The further distribution of files created by Amazon Elastic Transcoder may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining these licenses and paying any necessary royalties or fees.

32.2 We do not represent, warrant or guarantee the quality of any files you create through your use of Amazon Elastic Transcoder or that the files will be of a certain fidelity or error free.

33. AWS OpsWorks

33.1 You may use AWS OpsWorks to create a collection of AWS resources and provision them.

33.2 AWS may make sample templates available for you to use in connection with AWS OpsWorks. Sample templates may include chef recipes and/or sample code. All sample templates are offered “as is” and you are solely responsible for your use of the sample templates.

33.3. Any templates you use in connection with AWS OpsWorks must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

33.4. In addition to any charges you incur for your use of AWS Opsworks, you are responsible for all fees incurred for AWS services used in connection with AWS OpsWorks.

33.5. You may install and use the AWS Opsworks agent solely with AWS Opsworks. Your use of the AWS Opsworks agent is governed by the AWS Opsworks Client License Agreement, located here: [AWS Opsworks Client License Agreement](#).

34. AWS CloudHSM

34.1 You may not access, modify, update or tamper with, or attempt to access, modify, update or tamper with, any of the software installed on the HSM device, except as expressly permitted by us.

34.2 As part of the AWS CloudHSM service, AWS will provide access to HSM devices of its choosing. You have no ownership or rental rights in the specific HSM device to which we provide you access in the course of providing the AWS CloudHSM service.

34.3. In conjunction with the AWS CloudHSM service, you may be allowed to use certain software (including related documentation) developed and owned by SafeNet, Inc. or its licensors (collectively, the “SafeNet Software”). In connection with your use of the SafeNet Software, SafeNet and its licensors require that you agree to the additional terms and conditions located [here](#) .

34.4. If you elect to discontinue use of a HSM device, you must issue a command to delete the contents of the device (i.e., “zero-ize” the device). You will continue to be charged for use of an HSM device until the device has been zero-ized out and you notify us that you wish to discontinue the service.

34.5. Failure of an HSM device can result in unrecoverable data loss. We do not perform backups or implement fault tolerant configurations on your behalf. You are solely responsible for backup and fault tolerant configurations.

35. Amazon AppStream

35.1. When you use AppStream, you also use Amazon EC2, CloudWatch and AutoScaling, S3, and DynamoDB, and your use of AppStream is subject to all the terms that govern those services.

35.2. The software and other content that you upload to run on AppStream (including your AppStream hosted application, dependencies and installer), your AppStream entitlement service, and your AppStream client software are Your Content. The use of Your Content with AppStream, including the transmission of internet video and your distribution of any video decoder in your AppStream client software, may require that you obtain license rights from third parties. You are solely responsible for obtaining necessary licenses and paying any necessary royalties or fees applicable to Your Content.

35.3. Using NVIDIA Software. Use of the graphics processing unit (GPU) of an EC2 instance requires that you use driver software developed and owned by NVIDIA

Corporation or its licensors (collectively, the “NVIDIA Software”). If your AppStream application uses the GPU on an EC2 instance, NVIDIA and its licensors require that you agree to these additional terms and conditions:

- Your use of the NVIDIA Software is subject to the terms and conditions of the License for Customer Use of NVIDIA Software, currently located at <http://www.nvidia.com/content/DriverDownload-March2009/licence.php?lang=us> (the “NVIDIA License”). By using the NVIDIA Software, you hereby agree to be bound by the terms of the NVIDIA License.

35.4. We may collect information about Your Content’s use of AppStream, including CPU and GPU utilization, memory usage, IO performance, client type, client session length, transmission latency, client geographic and network locations, video and audio quality, and error and information messages.

35.5. AppStream Stand-Alone; AppStream Materials. We may make AppStream software and other materials (“AppStream Materials”) available to you on instances running in your own AWS account (“AppStream Stand-Alone”). AppStream Stand-Alone may only be used for your evaluation, development and testing purposes, and not for streaming your application to third party end users. AppStream Stand-Alone may enable you to direct us to pre-install certain third-party software on the instance via the applicable CloudFormation template. That third-party software may be subject to separate license terms and you are solely responsible for complying with those terms. AppStream Materials used on AppStream Stand-Alone are AWS Content and are subject to the license restrictions set out in the Agreement. You will only use the AppStream Materials on the AppStream Stand-Alone instance, and you will not download, transmit, or otherwise remove the AppStream Materials from AppStream Stand-Alone instances.

36. Amazon WorkSpaces

36.1. Any Content that you or any End User run on, cause to interface with, or upload to your WorkSpaces is Your Content. You are responsible for maintaining licenses and adhering to the license terms of any of Your Content on your WorkSpaces.

36.2. Using Microsoft Software. In conjunction with the Services, you and your End Users may be allowed to use Microsoft Software. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to the additional terms and conditions specified in section 4.2 above.

36.3. You and End Users may only use the WorkSpaces Services for an End User’s personal or office productivity. WorkSpaces are not meant to accept inbound network connections, be used as server instances, or serve web traffic or your network traffic. You may not reconfigure the inbound network connections of your WorkSpaces. We may shut down WorkSpaces that are used in violation of this section or other provisions of the Agreement.

36.4. You and End Users may only use the WorkSpaces client software on computer equipment owned or controlled by you or your End Users for your internal business

purposes, solely to access Your Content used in connection with the Services. Your use of the WorkSpaces client software is governed by the WorkSpaces Client Software License Agreement located here: <http://help.amazonworkspaces.com/app-terms.html>.

36.5. As part of regular operation the Service will be able to perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks the Service will use programmatic access that is provisioned as part of the Workspace creation. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

36.6. The charges for the Service apply on a monthly basis. If a Workspace is launched after the first of a month, then the monthly price for that Workspace will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a Workspace is terminated before the end of a month, then the monthly charge will still apply.

36.7. The charges for the Service include the cost of streaming data between your WorkSpaces and End Users' devices unless you stream via VPN, in which case you will be charged VPN data transfer rates in addition to any applicable Internet data transfer charges. Other Workspace data transfer will be charged using Amazon EC2 data transfer pricing.

36.8. You may not attempt to tamper with any software we pre-load on the Workspace instance (including the operating system software running on the Workspace), or in a way that is not part of normal operations or that attempts to circumvent charges for the Service. During the regular operation of the Service, software installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with or use this license activation server in a way that is not part of normal operations or that attempts to circumvent charges for the Service. We may block access to the Service, and suspend your account, if we determine that you are in violation of this section.

36.9. As part of regular operation of the service, WorkSpaces may be updated with latest operating system and software patches. During such updates, only software, documents, and settings that are part of the OS image used for the Workspace or part of a user's profile (D: drive in the Workspace) will persist.

36.10. Microsoft BYOL Licensing. Under this option, Amazon WorkSpaces enables you to provision WorkSpaces using your Microsoft Software and Microsoft Licenses (the "WorkSpaces BYOL Program"). You must be eligible to use the WorkSpaces BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using Microsoft Software under the WorkSpaces BYOL Program, you agree to the Microsoft EULA. You agree that you have determined that your use of the WorkSpaces BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted. AWS recommends that you consult with your

own advisors to understand and comply with the applicable Microsoft licensing requirements.

36.11. You are responsible for End Users use of your WorkSpaces. You are responsible for determining End User policies and configuring End User policy controls for WorkSpaces.

37. Amazon Cognito

37.1 Any third party identity provider that you use in connection with Amazon Cognito is Third Party Content under the Agreement, and features of Amazon Cognito that depend on such identity providers may not be secure, uninterrupted or error-free. Your use of such an identity provider is subject to the provider's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change, discontinue, or deprecate support for an identity provider for any reason and at any time.

37.2 You are responsible for (a) providing legally adequate privacy notices to your end users; (b) obtaining any necessary consent from the end user for the collection, use, transfer, and storage of any name, password, other login information, or personally identifiable information or personal data of any end user that you (or any third-party plug-in or service provider you use) may access; (c) using and authorizing others to access and use the information only for the purposes permitted by the end user; and (d) ensuring the information is collected, used, transferred, and stored in accordance with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

38. Amazon WorkDocs

38.1 You will need an AWS account to start using the Service Offering. Once you have enabled Amazon WorkDocs under your account, End Users can be invited to join, sign up, and start using the Service Offering under your account without each one having a separate AWS account.

38.2 You are responsible for paying the fees for use by you and your End Users of the Service Offering associated with your AWS account.

38.3 Within the Service Offering, your End User accounts are managed by End Users with administrative privileges ("WorkDocs Administrators"). These WorkDocs Administrators can access information about the accounts of other End Users, such as when they last logged in, what documents they viewed, etc. These WorkDocs Administrators can also deactivate other End Users' accounts and control access to certain functionality, such as restricting the ability to share files with external domains or changing their storage limits.

38.4 We may limit the number of versions that you can store for each file. We will announce any change in limits to the number of versions that you may store in advance of implementing those limits.

38.5 We may delete, without liability of any kind, any of your End Users' data or Content uploaded to Amazon WorkDocs if the End User is marked "Inactive" in Amazon WorkDocs' Administrator Dashboard and has not been billed for more than 60 days. We may also delete your Amazon WorkDocs site and Content when you have no End Users marked "Active" within Amazon WorkDocs Administrator Dashboard for more than 60 days.

38.6 If no End User accounts associated with your AWS account have registered any usage of the Service Offering for several months, then we may delete the inactive End Users' accounts after providing 30 days' notice.

38.7 You and your End Users may not use the Service Offering to host any files that violate the AWS Acceptable Use Policy. If we determine, in our sole discretion, that your use of the Service Offering may be in violation of the AWS Acceptable Use Policy or the Agreement, then we may delete those files.

38.8 Your use of the Amazon WorkDocs Sync Software is governed by the Amazon WorkDocs Sync License Agreement found here:[Amazon WorkDocs Sync License Agreement](#) .

38.9 Your use of an Amazon WorkDocs Application is governed by the Amazon WorkDocs Application License Agreement found here:[Amazon WorkDocs Application License Agreement](#) .

38.9 Your use of the Amazon WorkDocs Web Clipper is governed by the Amazon WorkDocs Web Clipper License Agreement found here:[Amazon WorkDocs Web Clipper License Agreement](#) .

39. Mobile Analytics

39.1 Your Data; Privacy. You are solely responsible for all information and data you collect or store using Mobile Analytics ("Your Data"). Your Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your Data (including by us), and (b) collect, use, transfer, and store Your Data in accordance with any privacy notice you provide, and all applicable laws.

40. AWS Config

40.1 You are responsible for all fees incurred for Services, such as Amazon SNS and Amazon S3, used in connection with AWS Config.

41. AWS CodeDeploy

41.1 AWS CodeDeploy to Amazon EC2 instances is offered at no additional charge but requires the use of other AWS Services. AWS CodeDeploy to on-premises instances is offered at the then current fees and charges that are posted on the AWS CodeDeploy detail page on the AWS Site; and may also be used with other AWS Services. You are responsible for all fees incurred for Services used in connection with AWS CodeDeploy.

41.2 AWS may make available reference or sample AppSpec configuration files and applications for you to use in connection with AWS CodeDeploy. These files and applications are provided “as is”, and you are solely responsible for your use of such files and applications. You will be charged the same fees for running them as you would be charged for running your own application.

42. AWS Lambda

42.1 You are responsible for Your Content, including (a) the performance of software you use with AWS Lambda and any reference libraries we provide and (b) maintaining licenses and adhering to the license terms of any software you run.

42.2 You are responsible for all fees incurred for Services used in connection with AWS Lambda.

42.3 We may delete, upon 30 days’ notice to you and without liability of any kind, any of Your Content uploaded to AWS Lambda if it has not been run for more than three (3) months.

43. Amazon WorkMail

43.1 The charges for the Service apply on a monthly basis. If an End User account is created after the first of a month, then the monthly fee for that mailbox will be adjusted on a pro rata basis from the first day it was active to the end of that month. If an End User account is terminated or deleted before the end of a month, then the monthly fee for that End User account will still apply. You are responsible for paying the fees for all End User accounts associated with your AWS account.

43.2 Amazon WorkMail allows you to register a test mail domain (e.g. <yourname>.awsapps.com). You can use the test mail domain as long as you are using Amazon WorkMail. If you stop using Amazon WorkMail, the test mail domain may become available to be registered and used by other Customers. You cannot use the test mail domain for other purposes outside of Amazon WorkMail.

43.3 If your use of Amazon WorkMail is terminated, we may delete your data and your End Users’ mailboxes.

43.4 When you use Amazon WorkMail, you also use AWS Key Management Service, AWS IAM, and Amazon SES, and your use of Amazon WorkMail is subject to the terms that govern those services. You are responsible for the separate fees you may accrue for using AWS Key Management Service.

43.5 Amazon WorkMail provides a filtering service designed to filter unwanted emails, such as spam, phishing emails, and email infected with viruses. You acknowledge that the technological limitations of the filtering service will likely result in the capture of some legitimate email, and the failure to capture some unwanted email, including email infected with viruses.

43.6 Your mail domain and End Users’ accounts may be blocked, delayed or prevented from being delivered by destination email servers and other reasons outside of our

control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed, or blocked.

43.7 You agree not to use Amazon WorkMail for sending:

- Bulk emails, such as mass marketing emails
- Unsolicited and unwanted emails
- Phishing emails

43.8 Your use and your End Users' use of Amazon WorkMail must comply with the AWS Acceptable Use Policy, applicable law, and the Agreement. You are solely responsible for understanding and complying with the legal and regulatory requirements applicable to your business. You are solely responsible for ensuring any emails you or your End Users send using Amazon WorkMail comply with the Federal CAN-SPAM Act and all other applicable law. You agree that AWS is not the "sender" of any emails you or your End Users send using Amazon WorkMail as defined in the Federal CAN-SPAM Act and all other applicable laws.

43.9 Amazon WorkMail may log and use information such as server hostnames, IP addresses, timestamps, mail queue file identifiers, and spam filtering information for the purpose of troubleshooting or improving Amazon WorkMail.

44. Amazon Machine Learning

44.1 You may only use Amazon Machine Learning ("Amazon ML") to process Your Content. You are solely responsible for the proper configuration of all security settings associated with Amazon ML.

44.2 We retain all rights to all improvements we make to any Amazon websites or technologies, including any and all improvements resulting from or related to Amazon ML processing Your Content.

44.3 We may delete, without liability of any kind, any Amazon ML object that remains inactive for more than the number of days specified in the user documentation.

44.4 You are responsible for all fees incurred from your use of Amazon ML regardless of the quality of the results obtained. Your use of Amazon ML requires the use of other Services. You are responsible for all fees incurred for Services used in connection with Amazon ML.

45. Amazon WorkSpaces Application Manager (Amazon WAM)

45.1 Any Content that you or any End User run on, cause to interface with, or upload to Amazon WorkSpaces Application Manager (Amazon WAM) via the Amazon WAM Admin Studio is Your Content.

45.2 You are responsible for maintaining licenses and adhering to the license terms of any of Your Content delivered via Amazon WAM to your WorkSpaces.

45.3 As part of regular operation of Amazon WAM, the Service will be able to perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks the Service will use programmatic access that is provisioned as part of Amazon WAM. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

45.4 As part of regular operation of Amazon WAM, the Service will use the End User and machine identity that is part of your AWS Directory Services environment to check for content that an End User is entitled to use. In addition, content installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with this license activation server, or use it in a way that is not part of normal operations or that attempts to circumvent this Service. We may block access to this Service, and suspend your account, if we determine that you are in violation of this Section.

45.5 The charges for the Service apply on a monthly basis. If Amazon WAM is enabled for an End User after the first of a month, then the monthly price for that End User's subscription will be adjusted on a pro rata basis from the first day it was active to the end of that month. If Amazon WAM is disabled for an End User before the end of a month, then the entire monthly charge will still apply.

45.6 When you use Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you may also use other AWS Services, and use of other AWS Services is subject to the terms that govern those Services. In addition to any charges you incur for your use of Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you are responsible for all fees incurred for AWS Services used in connection with Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications.

45.7 Amazon WAM Admin Studio, Amazon WAM Admin Player, and Amazon WAM desktop applications are AWS Content and may not be manipulated or reverse engineered in any way.

45.8 You may use the Amazon WAM Admin Studio only to package applications, and the Amazon WAM Admin Player only to validate applications, that will be delivered via Amazon WAM to your WorkSpaces. You may not tamper with either of those applications that we preload as part of the Amazon WAM Admin Studio or Player, the underlying Amazon EC2 AMI, or use the Amazon WAM Admin Studio or Player in a way that is not part of normal operations or that attempts to circumvent this Service.

45.9 You may not attempt to tamper with any software that is part of the Amazon WAM service that we preload on the Workspace instance, or use it in a way that is not part of normal operations or that attempts to circumvent this Service.

45.10 As part of regular operation of the Service, we may update Amazon WAM desktop applications with software patches.

45.11 You are responsible for End Users use of Amazon WAM. You are responsible for determining End User policies and configuring End User policy controls for using applications via Amazon WAM.

46. AWS Marketplace for Desktop Apps

46.1 The AWS Marketplace for Desktop Apps is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may be sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content.

46.2 Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

46.3 AWS may stop providing the AWS Marketplace for Desktop Apps (or any features of or listings within the AWS Marketplace for Desktop Apps) to you at AWS's sole discretion, without prior notice to you. In addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

46.4 You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace for Desktop Apps. This may include one-time payments as well as recurring payments. A "recurring payment" is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g., annually or monthly). The applicable charge for the Content is listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. If a subscription is purchased after the first of a month, then the monthly price for that Content will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a subscription is cancelled before the end of a month, then the entire monthly charge will still apply. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

46.5 Third-party support information for each subscription, if any, is set forth on the detail page for the Content. While AWS may help facilitate the resolution of disputes between you and third-party Content creators, for the Content, AWS does not guarantee the quality, safety or legality of items advertised, and support for the Content is the obligation of the third-party Content creator.

46.6 If the Content is offered, sold, or resold by AWS, then it is subject to the terms on the Content's detail page. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content offered or sold by third parties through the AWS Marketplace for Desktop Apps constitutes "Third Party Content" under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth

or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

47. AWS Directory Service

47.1 In conjunction with your use of AWS Directory Service, you and your End Users may be allowed to use Microsoft Software. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to the additional terms and conditions specified in Section 4.2 above.

47.2 If your AWS account is suspended for sixty (60) days or more, we may delete, without liability of any kind, Your Content and directories that are stored in AWS Directory Service upon thirty (30) days prior notice to you.

47.3 We may terminate your AWS Directory Service directory instance if you attempt to access, tamper with, or modify any software or configuration we pre-load on the directory instance, including the operating system software running on the directory instance.

48. Amazon API Gateway

48.1 You may use the Amazon API Gateway to publish, maintain, monitor, and secure Your Content at any scale to accept and process concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.

48.2 By using the Amazon API Gateway you acknowledge and agree that established throttling thresholds may vary, cache services may be limited by us in our sole discretion, and version capacity will not exceed 300 deployments per API at any given time. In addition and without limiting your obligations under the Agreement, you agree not to and not to attempt to: (i) access any resources not assigned to you by us; and/or (ii) perform any form of network discovery and/or load testing of Your Content inside the Amazon API Gateway.

48.3 You are solely responsible for the access, operation, performance, and security of all Your Content you use with Amazon API Gateway.

49. AWS Device Farm

49.1 As part of the AWS Device Farm, you may provide us with application package(s), test package(s) (pre-compiled), test script source code, application extension files, and/or auxiliary data files that have been developed by or for you in a format specified by AWS (each, an “App” or “Apps”) for testing on one or more mobile devices, tablets or other devices that we make available through the AWS Device Farm (each, a “Device(s)”). You may select one or more tests in the AWS Device Farm to be performed with your App(s) on the Device(s) you select (a “Test” or “Testing”).

49.2 For any Test run on an Apple Device (each, an “Apple Test”), you represent and warrant that you have an active and valid registered Apple Developer Account under the iOS Developer Program License Agreement with Apple at the time any such Apple Test

is run. You appoint us as your Authorized Developer (as defined in the iOS Developer Program License Agreement) for the duration of all Apple Tests and understand that you are responsible to Apple for all actions we undertake in connection with each Apple Test.

Without limiting your obligations under the Agreement, you agree not to and not to attempt to:

- (i) perform any network discovery inside the AWS Device Farm or otherwise in connection with the Test;
- (ii) access any resources not assigned to you by us (including any Devices);
- (iii) generate any internet traffic from within the EC2 instances of AWS Device Farm, unless approved by us; internet traffic should be limited to Devices only;
- (iv) attempt to establish a direct connection to any Device, nor access or connect to other infrastructure components except as permitted by us;
- (v) root, unlock, or jailbreak any Device;
- (vi) modify any files generated by the AWS Device Farm in a manner that would interfere with any Services;
- (vii) install persistent software on Devices or EC2 instances; and/or
- (viii) factory reset or change settings on Devices nor call and/or access third-party servers in a manner that would interfere with any Services.

49.3 You agree not to rely on any Testing or Report for any purpose, including that any App(s) meet any requirements for inclusion in any application repository of any kind (such as the Apple App Store or Google Play Store). You acknowledge and agree that we may disclose the App(s) to third parties solely for purposes of conducting automated security verification.

49.4 We make no representation as to the availability of the AWS Device Farm. We may change the Tests, Reports or Device(s) offering(s) or any other components or services that are a part of or available through the AWS Device Farm at any time.

50. Amazon Elasticsearch Service

50.1 Amazon Elasticsearch Service creates daily automated snapshots of your Amazon Elasticsearch Service domains. We will maintain these automated snapshots for a period of 14 days after they are created. We may delete automated snapshots, without liability of any kind, at any time after 14 days.

50.2 You may not access or tamper with any software we install on the Amazon Elasticsearch Service domains.

50.3 We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the Amazon Elasticsearch Service domains.

51. AWS Database Migration Service and AWS Schema Conversion Tool

51.1 You may use AWS Database Migration Service solely for the purpose of migrating data to or from Amazon RDS or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the “DMS Supported Services”). Neither you nor any End User may use the Amazon RDS Migration Service to migrate data, directly or indirectly, from a source that is not a DMS Supported Service to a destination that is also not a DMS Supported Service.

51.2 AWS Database Migration Service and the AWS Schema Conversion Tool collect non-personally identifiable metrics regarding your use of the Service Offerings, including the types of database engines used, number of rows processed, duration of the migration or conversion tasks, and migration or conversion task failure status. These metrics may be used by AWS to provide, maintain, and improve the quality and feature set of the Service Offerings.

51.3 The AWS Schema Conversion Tool is AWS Content, and you may install and use it solely for the purpose of migrating your database schemas to Amazon RDS or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the “SCT Supported Services”). Neither you nor any End User may distribute the AWS Schema Conversion Tool or use it to migrate database schemas to a destination that is not an SCT Supported Service. If you would like to use the AWS Schema Conversion Tool to migrate database schemas to a destination that is not an SCT Supported Service, contact us for special pricing.

51.4 AWS Database Migration Service is offered as a preview and is considered a Beta Service, as defined in these Service Terms. Your use of AWS Database Migration Service is subject to the Beta Service Participation terms, as described above.

52. Amazon Inspector

52.1 Amazon Inspector is AWS Content. Neither you nor any End User may, or may attempt to, distribute Amazon Inspector.

52.2 Some components of Amazon Inspector are governed by open source software licenses identified in the notice file accompanying the Amazon Inspector Agent. Your license rights with respect to these individual components are defined by the applicable open source software license.

52.3 Amazon Inspector is offered in a limited preview and is considered a Beta Service as defined in these Service Terms. Your use of Amazon Inspector is subject to the Beta Service Participation terms, as described above.

53. AWS Mobile Hub

53.1 AWS Mobile Hub can be used by you to connect to AWS Service Offerings as made available from time to time by AWS in its sole discretion. Use of the AWS Mobile Hub is subject to AWS Service Offering terms and applicable pricing. You are responsible for maintaining licenses and adhering to the license terms of any software you download and use in connection with AWS Mobile Hub.

54. AWS IoT

54.1 AWS IoT Services that you enable must comport with AWS IoT Developer Guidelines and this Agreement. AWS Developer IoT Guidelines are subject to change at any time without notice.

54.2 The following data guidelines currently apply to Registry and Shadow Data (as referenced in the AWS IoT Developer Guidelines) stored in connection with individual devices and may be changed at any time without notice. Device Shadow Data for an individual device expires and will be deleted if you do not update the Shadow Data for an individual device within 1 year (12 months). Device Registry Data for an individual device expires and will be deleted if you do not update the Registry data for an individual device within 7 years (84 months). Once the Registry and/or Shadow Data has been updated for an individual device the data restriction time frame for an individual device resets and the Registry and/or Shadow Data storage time frame for an individual device starts over.

54.3 You are responsible for all applicable fees associated with use of the Services in connection with AWS IoT. You are solely responsible, and we have no liability, for any activities that occur in the application and/or use of AWS IoT, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of any AWS IoT devices enabled by your AWS account.

55. Amazon QuickSight

55.1 You may enable End Users to use Amazon QuickSight under your account. Termination of your use of Amazon QuickSight, will also terminate such End Users' use of Amazon QuickSight.

55.2 Amazon QuickSight End User accounts are managed by End Users with administrative privileges ("Amazon QuickSight Administrators"). Amazon QuickSight Administrators can (a) activate and deactivate End Users' Amazon QuickSight accounts; (b) control End User access to data sets and certain functionality of Amazon QuickSight; and (c) access information about End Users' use of Amazon QuickSight.

55.3 Amazon QuickSight may use Your Content to make personalized recommendations to you, such as suggested visualizations based on your query history.

55.4 Subject to the Agreement and these Service Terms, you and your End Users may use Amazon QuickSight by logging into quicksight.aws.amazon.com.

55.5 Amazon QuickSight is offered as a preview and is considered a Beta Service, as defined in these Service Terms. Your use of Amazon QuickSight is subject to the Beta Service Participation terms, as described above.

56. AWS Certificate Manager

56.1 By using AWS Certificate Manager (“ACM”) you authorize us, Amazon Trust Services, LLC (“ATS”), or our affiliates (collectively, “Amazon CA”) to apply for and obtain SSL/TLS certificates (each, a “Certificate”) from certification authorities, some of whom may be third parties, for the domain name you provide to us. By submitting a request for a Certificate, you certify that (1) you are the Domain Name Registrant (as defined in the then current CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (the “CA/B Forum Requirements” currently located at <https://cabforum.org/baseline-requirements-documents/>)); (2) you have control over the Fully-Qualified Domain Name (as defined in the CA/B Forum Requirements); or that (3) you have been granted authority by the Domain Name Registrant to authorize Amazon CA to apply for and obtain each Certificate. You acknowledge that, solely for purposes of obtaining the Certificate and for no other purposes, you are giving Amazon CA control over the Fully-Qualified Domain Name, and you approve of it requesting the Certificate for the domain name. We may decline to provide you with a Certificate for any reason.

56.2 You agree that:

- i. All information you provide in connection with your use of ACM is and will be accurate and complete information at all times (and you will promptly notify us if your information changes);
- ii. You will review and verify the Certificate contents for accuracy;
- iii. You may use a Certificate provided to you by us solely on servers that are accessible at the subjectAltName(s) listed in the Certificate and will use the Certificate solely in compliance with all applicable laws;
- iv. You will promptly cease using a Certificate, and promptly notify us, in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
- v. You will promptly cease using a Certificate, and promptly notify us, if the private key associated with the Certificate is, or becomes, subject to a Key Compromise (as defined in the CA/B Forum Requirements) or the Certificate is otherwise subject to misuse;
- vi. You will promptly respond to Amazon CA’s instructions concerning Key Compromise or Certificate misuse;
- vii. You will not modify, sublicense, or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or private key;

- viii. You will not, in connection with use of the Certificate, upload or distribute any files or software that may damage the operation of another's computer;
- ix. You will not make representations about or use a Certificate except as may be allowed in ATS's [CPS](#) ;
- x. You will not, in connection with use of the Certificate, impersonate or misrepresent your affiliation with any entity;
- xi. You will not permit an entity other than Amazon CA to control the Private Key matching the Public Key in the Certificate (where "Private Key" and "Public Key" are defined by the CA/B Forum Requirements);
- xii. You will not use a Certificate to breach the confidence of a third party or to send or receive unsolicited bulk correspondence; and
- xiii. Notwithstanding anything to the contrary in the Agreement, you acknowledge that Amazon CA (or our applicable third-party contractor) may revoke a Certificate at any time, and you agree that you will cease using the Certificate immediately upon our notice of such revocation.

57. Amazon Lumberyard Engine

57.1 Lumberyard Materials. Amazon Lumberyard consists of an engine, integrated development environment, and related assets and tools we make available at aws.amazon.com/lumberyard/downloads or otherwise designate as Lumberyard materials (collectively, "Lumberyard Materials"). The Lumberyard Materials include the "Lumberyard Redistributables" listed at docs.aws.amazon.com/console/lumberyard/userguide/lumberyard-redistributables . Lumberyard Materials are AWS Content. The term "Lumberyard Materials" does not include Content distributed with the Lumberyard Materials under separate license terms (such as code licensed under an open source license).

57.2 License. In addition to the rights granted to AWS Content under the Agreement, we also grant you a limited, non-exclusive, non-sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

a. Development: You may use, reproduce, modify, and create derivative works of the Lumberyard Materials to develop and support video games, software, audio-visual works, and other content (each work created through use of the Lumberyard Materials is a "Lumberyard Project"). Lumberyard Projects, excluding any AWS Content and Third Party Content included therein, are Your Content.

b. Distribution to End Users: You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute (including via third party distributors) to End Users the Lumberyard Redistributables (including any permitted modifications and derivatives) as part of a Lumberyard Project. However, you may do so only if (i) the Lumberyard Project provides material content or functionality beyond that provided by

the Lumberyard Redistributables themselves, (ii) the Lumberyard Redistributables are integrated into the Lumberyard Project so they are not separately usable by End Users, (iii) you do not distribute in source code form Lumberyard Redistributables that we make available in file formats that are commonly compiled (e.g., C, C++) or for which we make a compiler available, and (iv) you ensure End Users are subject to terms no less protective of the Lumberyard Materials than these Service Terms, including this Section and Sections 57.4 and 57.5 below. You may sublicense these rights, subject to the restrictions in these terms, to your End Users to allow them to use, modify, create new content for, and redistribute your Lumberyard Project (e.g., create new items or levels for a game).

c. Collaboration with other AWS Customers. You may reproduce and distribute (but not sublicense) the Lumberyard Materials (including any permitted modifications and derivatives) (i) to other AWS customers that are contractors of yours solely for the purpose of allowing those AWS customers to perform work on your behalf, (ii) to other AWS customers in connection with work you perform for them as a contractor, and (iii) to up to 5 other AWS customers who you authorize to distribute a Lumberyard Project in connection with your sale or licensing of that Lumberyard Project (e.g., publishers of a game you develop). Those other AWS customers' rights to the Lumberyard Materials are governed by their agreement(s) with us.

57.3 No License Fee. There is no fee for the licenses granted in Section 57.2. Other Service Offerings and Third Party Content made available in connection with the Lumberyard Materials may be subject to separate charges and governed by additional terms.

57.4 Operating Restrictions. Without our prior written consent, (a) the Lumberyard Materials (including any permitted modifications and derivatives) may only be run on computer equipment owned and operated by you or your End Users, or on AWS Services, and may not be run on any Alternate Web Service and (b) your Lumberyard Project may not read data from or write data to any Alternate Web Service. "Alternate Web Service" means any non-AWS web service that is similar to or can act as a replacement for the services listed

[atdocs.aws.amazon.com/console/lumberyard/userguide/alternate-web-services](https://docs.aws.amazon.com/console/lumberyard/userguide/alternate-web-services) .

57.5 Other Restrictions. Without limiting the license restrictions set out in the Agreement, you may not (a) distribute the Lumberyard Materials in source code form, except as expressly permitted by Section 57.2(b) and (c), (b) use or exploit the Lumberyard Materials or any portion thereof to develop, maintain, participate in the development of, or support any competing engine, development tool, or software framework, (c) use the Lumberyard Materials or any portion thereof as part of a logo or trademark, (d) remove, obscure, or alter any proprietary rights notices (including copyright and trademark notices) contained in the Lumberyard Materials, (e) take any action that would require us or you to license, distribute, or otherwise make available to anyone the Lumberyard Materials under different terms (e.g., combining Lumberyard Materials with software subject to "copyleft" open source licenses), or (f) use or exploit

the Lumberyard Materials or any portion thereof in any manner or for any purpose other than as expressly permitted by these terms.

57.6 Registration; Release. Before distributing your Lumberyard Project to End Users, you must register it at aws.amazon.com/lumberyard/registration. You must obtain our prior written consent if the initial public or commercial release of your Lumberyard Project is based on a version of the Lumberyard Materials more than 5 years old.

57.7 Credit. You must credit us in Lumberyard Projects in accordance with the guidelines located at aws.amazon.com/lumberyard/logo-guidelines. AWS Marks included in the Lumberyard Materials may only be used in accordance with the Trademark Use Guidelines. We may use excerpts of publicly released promotional material from your Lumberyard Projects and related trademarks, service marks, trade names, and logos in connection with our marketing, advertisement, and promotion of Lumberyard.

57.8 Forums; Submissions. When discussing Lumberyard Materials in our forums or elsewhere, you may include up to 50 lines of source code from the Lumberyard Materials for the sole purpose of discussing that code. You must identify us as the source of the code. Content relating to Lumberyard Materials that you post or otherwise submit to developer discussion sites, sample code repositories, or other AWS or public forums (collectively, “Lumberyard Submissions”) constitute Your Submissions under the Agreement, and you grant (i) us a non-exclusive, worldwide, perpetual, irrevocable, transferrable, sublicensable, royalty-free, and fully paid up license under all intellectual property rights to your Lumberyard Submissions, and (ii) other AWS customers the same rights to your Lumberyard Submissions as these Service Terms provide to the Lumberyard Materials.

57.9 Data Collection. The Lumberyard Materials may provide us with information about the use of the Lumberyard Materials, including information about system and server resources, features used in the integrated development environment, frequency and duration of use, geographic and network locations, and error and information messages.

57.10 Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the [AWS Acceptable Use Policy](#). The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as use in operation of medical equipment, automated transportation systems, autonomous vehicles, aircraft or air traffic control, nuclear facilities, manned spacecraft, or military use in connection with live combat. However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.

57.11 Termination. Your rights in the Lumberyard Materials automatically terminate if the Agreement terminates or you breach the Agreement (including these Service Terms). However, if we terminate the Agreement for convenience, your rights in Lumberyard Materials then in your possession survive termination with respect to any

previously registered Lumberyard Project. Otherwise, upon termination, you must cease all use, distribution, and other exploitation of the Lumberyard Materials (and any modifications and derivatives).

58. Amazon GameLift.

58.1 Your Content. You are solely responsible for Your Content, including (a) the performance of software you use with Amazon GameLift and (b) maintaining licenses and adhering to the license terms of any software you run.

58.2 Other Services. When you use Amazon GameLift, you are also using Amazon EC2. Amazon EC2 and certain other Service Offerings and Third Party Content made available via Amazon GameLift are subject to separate charges and governed by additional terms.

58.3 Daily Active Users. Amazon GameLift fees are based in part on the number of your End Users that connect to Amazon GameLift. To allow us to accurately calculate your fees, you must provide us a unique, non-personally identifiable identifier for each of those End Users, as specified in the Amazon GameLift documentation.

58.4 Inactivity. We may delete, upon 30 days' notice to you and without liability of any kind, any of Your Content uploaded to Amazon GameLift if it has not been run for more than 3 months.

58.5 Your GameLift Data. Amazon GameLift may enable you to collect information and data from your End Users ("Your GameLift Data"). Your GameLift Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your GameLift Data, and (b) collect, use, transfer, and store Your GameLift Data in accordance with any privacy notice you provide and all applicable laws.

AWS PUBLIC SECTOR ACCESS POLICY

(Last Updated July 21, 2015)

This AWS Public Sector 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 8 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 be 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.

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 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the Services are provided (as applicable) to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the Services. If you are using the Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, 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. 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.

7. 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).

8. Definitions.

"Acceptable Use Policy" means the policy currently available at <http://aws.amazon.com/aup>, as it may be 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.

info|RELIANCE

STATE OF UTAH DIVISION OF PURCHASING NASPO VALUEPOINT CLOUD SOLUTIONS

SUBMITTED TO:

State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Mr. Christopher Hughes
Assistant Director
christopherhughes@utah.gov
(801) 538-3254

SUBMITTED BY:

InfoReliance Corporation
4050 Legato Road, Suite 700
Fairfax, VA 22033

Ms. Theresa Grouge
Director of Contracts
Theresa.grouge@infoeliance.com
(703) 246-9360, x1162 (phone)
(703) 246-9331 (fax)

Attachment I – Draft Ordering Instructions and Template

InfoReliance is proud to have been awarded a Master Agreement from NASPO ValuePoint to provide Cloud Infrastructure as a Service (IaaS) Solutions. Our full catalog includes 53 distinct offerings from our Fulfillment Partner Amazon Web Services (AWS). Value-added services in scope under the Master Agreement include service provisioning, billing and invoicing, identity and access management, reporting, 24x7x365 Enterprise Service Desk support, and training.

Additionally, we offer optional related services including systems engineering and configuration, cloud migration, custom application development, cloud consulting, network and database administration, cloud single sign on, disaster recovery, and Big Data and analytics. These are available as established in each Participating Entity's negotiated Participating Addendum.

InfoReliance Corporation Ordering Instructions

InfoReliance Corporation Ordering Instructions	
Master Agreement Number	[TBD on award]
Contract Type	Catalog pricing with two percent (2%) minimum discount off list
Contract Duration	10 years
Authorized Buyers	All NASPO Participating Entities may negotiate a Participating Addendum under this Master Agreement.
Scope	The Master Agreement contract provides Participating Entities with access to technical capabilities that run in cloud environments and meet the NIST Essential Characteristics. All InfoReliance offerings are classified as Infrastructure as a Service (IaaS), meet the NIST definition of Cloud Computing, and are open to all deployment models (private, public, community, or hybrid).
CAGE Code	1Q4A0
DUNS Number	143147762
Federal TIN	54-1979520
Address	InfoReliance Corporation 4050 Legato Road, Suite 700 Fairfax, VA 22033
Payment Terms	Net 30 Days
Payment Information	PNC Bank Checking Account Number: 5303792351 ABA/Routing Number: 054000030
Warranty	Standard Commercial Warranty included; Extended Warranty and Customized Options Available
To obtain a quote for cloud services	naspo@infoeliance.com
To receive policy and procedural information regarding installation, basic warranty, extended warranty, technical support, software support and other post-delivery issues	naspo@infoeliance.com You may also contact AWS Business Support directly through your AWS account for access to AWS Cloud Support engineers.
To troubleshoot a problematic order	naspo@infoeliance.com
Links to Related Web Sources	Sales and Ordering: https://www.infoeliance.com/naspo AWS Calculator: http://calculator.s3.amazonaws.com/index.html AWS Product Documentation: https://aws.amazon.com/products

InfoReliance Corporation Contact Information

InfoReliance Corporation Contact Information	
Customer Service Desk	[Toll free number to be established after award] naspo@infoeliance.com
NASPO Contract Manager	Ms. Theresa Grouge 703-246-1162 (Phone) 703-246-9331 (Fax) theresa.grouge@infoeliance.com
NASPO Contract Administrator	Ms. Athena Partik 703-246-9360 x1647 athena.partik@infoeliance.com
NASPO Usage Report Administrator	Ms. Lauren Gardner 703-278-7735 lauren.gardner@infoeliance.com
Executive Sponsor	Mr. John Sankovich 703.246.9360 x1115 john.sankovich@infoeliance.com
Director of Sales Operations	Mr. Steven Johnson 703-460-2057 steven.johnson@infoeliance.com
Sales Operations Manager	Mr. Daniel Archer 703-278-7721 daniel.archer@infoeliance.com

Sample NASPO Ordering Template/Input Form

NASPO RFQ #: (if applicable use ValuePoint eMarket Center number)		
Request Date: dd/mm/yyyy	Reply By Date: dd/mm/yyyy	00:00 AM/PM ET
Subject:		
Request Type: Request For Quote		
State/Local/Education/Agency Name:	POC First Name:	
	POC Last Name:	
Fax #:	E-mail:	
Street:		
City:	State:	Zip:
NASPO Contract Holder	Contract #	
InfoReliance Corporation	TBD on award	
Attachment (if required for parts, details or scope):		
Requirements: Provide a description of products or services required with details to properly provide a quote.		

AWS PUBLIC SECTOR ACCESS POLICY

(Last Updated July 21, 2015)

This AWS Public Sector 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 8 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 be 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.

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 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the Services are provided (as applicable) to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the Services. If you are using the Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, 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. 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.

7. 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).

8. Definitions.

"Acceptable Use Policy" means the policy currently available at <http://aws.amazon.com/aup>, as it may be 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.

AWS Service Terms

Last updated: February 22, 2016

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the [AWS Customer Agreement](#) or other agreement with us governing your use of our Services (the “Agreement”), the terms and conditions of these Service Terms apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

1. Universal Service Terms (Applicable to All Services)

1.1. You may only use the Services to store, retrieve, query, serve, and execute Your Content that is owned, licensed or lawfully obtained by you. As used in these Service Terms, “Your Content” includes any “Company Content” and any “Customer Content”. As part of the Services, you may be allowed to use certain software (including related documentation) provided by us or third party licensors. This software is neither sold nor distributed to you and you may use it solely as part of the Services. You may not transfer it outside the Services without specific authorization to do so.

1.2. You must comply with the current technical documentation applicable to the Services (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site. In addition, if you create technology that works with a Service, you must comply with the current technical documentation applicable to that Service (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site.

1.3. You will provide information or other materials related to Your Content (including copies of any client-side applications) as reasonably requested by us to verify your compliance with the Agreement. We may monitor the external interfaces (e.g., ports) of Your Content to verify your compliance with the Agreement. You will not block or interfere with our monitoring, but you may use encryption technology or firewalls to help keep Your Content confidential. You will reasonably cooperate with us to identify the source of any problem with the Services that we reasonably believe may be attributable to Your Content or any end user materials that you control.

1.4. If we reasonably believe any of Your Content violates the law, infringes or misappropriates the rights of any third party or otherwise violates a material term of the Agreement (including the documentation, the Service Terms, or the [Acceptable Use Policy](#)) (“Prohibited Content”), we will notify you of the Prohibited Content and may request that such content be removed from the Services or access to it be disabled. If you do not remove or disable access to the Prohibited Content within 2 business days of our notice, we may remove or disable access to the Prohibited Content or suspend the Services to the extent we are not able to remove or disable access to the Prohibited Content. Notwithstanding the foregoing, we may remove or disable access to any Prohibited Content without prior notice in connection with illegal content, where the

content may disrupt or threaten the Services, pursuant to the Digital Millennium Copyright Act or as required to comply with law or any judicial, regulatory or other governmental order or request. In the event that we remove content without prior notice, we will provide prompt notice to you unless prohibited by law.

1.5. From time to time, we may offer free or discounted pricing programs covering certain usage of the Services (each, a “Special Pricing Program”). We may stop accepting new sign-ups or discontinue a Special Pricing Program at any time. Standard charges will apply after a Special Pricing Program ends or if you exceed the limitations by the Special Pricing Program. You must comply with any additional terms, restrictions, or limitations (e.g., limitations on the total amount of usage) for the Special Pricing Program as described in the offer terms for the Special Pricing Program or on the pricing page for the eligible Service(s). You may not access or use the Services in a way intended to avoid any additional terms, restrictions, or limitations (e.g., establishing multiple AWS accounts in order to receive additional benefits under a Special Pricing Program), and we may immediately terminate your account if you do so. Any data stored or instances provided as part of a Special Pricing Program must be actively used.

1.6. If we make multiple discounts or pricing options for a Service available to you at one time, you will only be eligible to receive one discount or pricing option, and will not be entitled to cumulative discounting and pricing options.

1.7. You will ensure that all information you provide to us via the AWS Site (for instance, information provided in connection with your registration for the Services, requests for increased usage limits, etc.) is accurate, complete and not misleading.

1.8. From time to time, we may apply upgrades, patches, bug fixes or other maintenance to the Service Offerings (“Maintenance”). We agree to use reasonable efforts to provide you with prior notice of any scheduled Maintenance (except for emergency Maintenance) and you agree to use reasonable efforts to comply with any Maintenance requirements that we notify you about.

1.9 If your Agreement does not include a provision on AWS Confidential Information, and you and AWS do not have an effective non-disclosure agreement in place, then you agree that you will not disclose AWS Confidential Information (as defined in the AWS Customer Agreement), except as required by law.

1.10 Beta Service Participation

1.10.1. This Section describes the additional terms and conditions under which you may access and use certain features, technologies and services made available to you by AWS that are not yet generally available, including, but not limited to, any products, services, or features labeled “beta”, “preview”, “pre-release”, or “experimental” (each, a “Beta Service”) or access and use Service Offerings available in AWS regions that are not generally available, including, but not limited to, any AWS regions identified by AWS as “beta”, “preview”, “pre-release”, or “experimental” (each, a “Beta Region”). In the event there is a conflict between the terms of this Section 1.10 and an existing AWS

Beta Test Participation Agreement between you and AWS, the terms of the existing AWS Beta Test Participation Agreement will take precedence.

1.10.2. During the term of the applicable Beta Service or Beta Region (as specified by AWS), you may: (a) access and use the Beta Service or Service Offerings in any Beta Region solely for internal evaluation purposes; and (b) install, copy, and use any related AWS Content that may be provided to you by AWS in connection with the Beta Service or Service Offerings in any Beta Region (“Beta Materials”) solely as necessary to access and use the Beta Service or Service Offerings in any Beta Region in the manner permitted by this Section.

1.10.3. You agree not to allow access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials by any third party other than your employees and contractors who (i) have a need to use or access the Beta Service, Service Offerings in the Beta Region or Beta Materials in connection with your internal evaluation activities, and (ii) have executed written non-disclosure agreements obligating them to protect the confidentiality of non-public information regarding the Beta Service, Beta Region and Beta Materials.

1.10.4. You must comply with all policies and guidelines related to any Beta Service or Beta Region as posted on the AWS Site or otherwise made available to you, including the Privacy Policy, Acceptable Use Policy, the Service Terms, and any additional terms and conditions for a specific Beta Service or Beta Region. AWS may add or modify restrictions, including lowering or raising any usage limits, related to access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials at any time. If requested by AWS, you will promptly increase or decrease your usage of the applicable Beta Service, Service Offerings in a Beta Region or Beta Materials to the levels that AWS may specify. Service Level Agreements do not apply to Beta Services or any Services Offerings in Beta Regions.

1.10.5. AWS may suspend or terminate your access to or use of any Beta Service or Service Offerings in any Beta Region at any time and for any reason. AWS may at any time cease providing any or all of any Beta Service or any Service Offering in a Beta Region in its sole discretion and without notice. Beta Services and Services Offerings in Beta Regions also may be unavailable and/or their performance may be negatively affected by scheduled and unscheduled maintenance. AWS will use reasonable efforts to notify you in advance of scheduled maintenance, but AWS is unable to provide advance notice of unscheduled or emergency maintenance.

1.10.6. In consideration of being allowed to access and use a Beta Service or Service Offering in a Beta Region, you agree to provide AWS with information relating to your access, use, testing, or evaluation of the Beta Service, Service Offerings in the Beta Region or any related Beta Materials, including observations or information regarding the performance, features and functionality of the Beta Service or any related Beta Materials as applicable, when and in the form reasonably requested by AWS (“Test Observations”). AWS will own and may use and evaluate all Test Observations for its own purposes. You will not use any Test Observations except for your internal evaluation purposes of the Beta Service or Beta Region.

1.10.7. Each individual Beta Service and Service Offering in a Beta Region will automatically terminate upon the release of a generally available version of the applicable Beta Service or Service Offering in a Beta Region or upon notice of termination by AWS. Notwithstanding anything to the contrary in the Agreement or these Services Terms, either you or AWS may terminate your participation in a Beta Service or Service Offering in a Beta Region at any time for any reason upon notice to the other party. Notwithstanding anything to the contrary in the Agreement, after the conclusion of your participation in a Beta Service or Service Offering in a Beta Region for any reason, (a) you will not have any further right to access or use the applicable Beta Service or Service Offering in the Beta Region and Beta Materials; (b) your Content used in the applicable Beta Service or Service Offering in the Beta Region may be deleted or inaccessible; and (c) you will immediately return or, if instructed by AWS, destroy all Beta Materials or any other AWS Confidential Information related to the applicable Beta Service, Service Offering in any Beta Region or Beta Materials. If AWS releases a generally available version of a Beta Service or a Service Offering in a Beta Region, your access to and use of the generally available version will be subject to the Agreement and any separate Section of these Service Terms as may be specified for that generally available Service Offering. If any Beta Region becomes generally available, your access to and use of Service Offerings in the generally available AWS region will be subject to the terms and conditions applicable to that AWS region. AWS does not guarantee that any Beta Service or Service Offering in any Beta Region will ever be made generally available, or that any generally available version will contain the same or similar functionality as the version made available by AWS during the term of the Beta Service or Beta Region, as applicable. AWS does not guarantee that any Beta Region will become generally available.

1.10.8. Beta Materials, Test Observations, Suggestions concerning a Beta Service or Beta Region, or any other information about or involving (including the existence of) any Beta Service or Beta Region are considered AWS Confidential Information. You will not disclose (including, but not limited to, in a press release or public statement) any Beta Materials, Test Observations, Suggestions concerning a Beta Service, or any other information about or involving (including the existence of) any Beta Service, except as agreed by AWS in writing.

1.10.9. ADDITIONAL WARRANTY DISCLAIMERS. WITHOUT LIMITING ANY DISCLAIMERS IN THE AGREEMENT OR THE SERVICE TERMS, THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS ARE NOT READY FOR GENERAL COMMERCIAL RELEASE AND MAY CONTAIN BUGS, ERRORS, DEFECTS OR HARMFUL COMPONENTS. ACCORDINGLY, AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT OR THESE SERVICES TERMS, AWS IS PROVIDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS AND BETA MATERIALS TO YOU "AS IS." AWS AND ITS AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS, INCLUDING ANY WARRANTY THAT THE BETA SERVICES, SERVICE

OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS AND ITS AFFILIATES AND 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. AWS' AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY FOR ANY BETA SERVICES WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE BETA SERVICES THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

1.10.10. Because the Beta Services and Materials involve features, technologies and services that are not yet generally available, you acknowledge that any violation of this Section 1.10 could cause irreparable harm to AWS for which monetary damages may be difficult to ascertain or an inadequate remedy. You therefore agree that AWS will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Section 1.10.

2. Amazon CloudFront

2.1. You must own or have all necessary rights to use any domain name or SSL certificate that you use in conjunction with Amazon CloudFront. You are solely responsible for the renewal, security and proper configuration of any SSL certificates that you provide for use with Amazon CloudFront, including any disclosure of your SSL certificates to third parties.

2.2. Amazon CloudFront requires you to store the original version of Your Content in an origin server (such as Amazon S3). If you use other Services to store the original version of Your Content, you are responsible for the separate fees you accrue for the other Services and for Amazon CloudFront.

2.3. While you will only be charged fees specified for the selected Price Class, Your Content you select for delivery from edge locations in a Price Class may from time to time be served from edge locations located outside the regions in that Price Class.

2.4. Amazon CloudFront's Geo Restriction feature may utilize a third party geo-location database, which may not be accurate in all situations.

3. Amazon Simple Queue Service (Amazon SQS)

3.1. You may not knowingly create and maintain inactive queues. We may delete, without liability of any kind, any of Your Content that sits in an Amazon SQS queue or any Amazon SQS queue that remains inactive for more than the number of days specified in the user documentation.

4. Amazon Elastic Compute Cloud

4.1. In connection with your use of Amazon Elastic Compute Cloud (including all instances and instance types, hosts and other resources, dedicated, reserved or on-demand, collectively “Amazon EC2”) and the Services, you are responsible for maintaining licenses and adhering to the license terms of any software you run.

4.2. Using Microsoft Software. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the “Microsoft Software”). If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, “High Risk Use”). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- Microsoft is an intended third-party beneficiary of this Section 4.2, with the right to enforce its provisions.

4.3. Using Novell Software. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Novell, Inc. or its licensors (collectively, the “Novell Software”). If you choose to use the Novell Software, Novell and its licensors require that you agree to these additional terms and conditions:

- Your use of the Novell Software is subject to the terms and conditions of the Novell End User License Agreement (“Novell EULA”) provided with the Novell Software. By using the Novell Software, you hereby agree to be bound by the terms of the applicable Novell EULA, which is presented the first time you access the relevant machine image.

4.4. Using Red Hat Software. In conjunction with the Services, you may be allowed to use certain software (including related support, maintenance, and documentation) developed, owned or provided by Red Hat, Inc. or its licensors (collectively, the “Red Hat Software”). If you choose to use the Red Hat Software, Red Hat and its licensors require that you agree to these additional terms and conditions:

- Red Hat disclaims any (i) warranties with respect to the Red Hat Software and (ii) liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from your use of the Red Hat Software.
- Your use of the Red Hat Software is subject to the terms and conditions of the Red Hat Cloud Software Subscription Agreement currently located at www.redhat.com/licenses/cloud_cssa/ (the “Red Hat CSSA”). By using the Red Hat Software, you hereby agree to be bound by the terms of the Red Hat CSSA.

4.5. Spot Instance Pricing. You may request that certain Amazon EC2 instances run pursuant to the Spot instance pricing and payment terms (“Spot Instance Pricing”) set forth on the Amazon EC2 product detail page on the AWS Site (each requested instance, a “Spot Instance”). You must request Spot Instances through the AWS Management Console or by using API tools (“Spot Instance Request”). As part of your Spot Instance Request, you must specify the maximum hourly price you are willing to pay to run the requested Spot Instances (“Your Maximum Price”). Unless you specify a permissible alternative termination date, your Spot Instance Request will remain active until we fulfill it or you cancel it. We set the price for Spot Instances (the “Spot Price”), which may vary over time based on a number of factors, including the amount of available compute capacity we have available and the price you and other customers are willing to pay for Spot Instances (e.g., supply and demand). While a requested Spot Instance remains running, you will be charged the current Spot Price in effect at the beginning of each instance hour. You will not be charged more than Your Maximum Price. We may terminate Spot Instances at any time and without any notice to you if we determine the current Spot Price equals or exceeds Your Maximum Price or for AWS capacity requirements. If we terminate your Spot Instance, you will only be charged for each full hour the Spot Instance ran. AWS may allow you to purchase Spot Instances of a fixed duration (each, a “Spot Block”), where the Spot Price for that Spot Instance (the “Block Price”) will remain constant for the duration of the Spot Block, and you will be charged the Block Price for the duration of your Spot Block. Spot Instances purchased as Spot Blocks run independently of the Spot Price, and will not be terminated because the Spot Price equals or exceeds Your Maximum Price. Spot Instances purchased as Spot Blocks may still be terminated for AWS capacity requirements and will terminate at the conclusion of the fixed duration. If a Spot Instance purchased as a Spot Block is terminated due to AWS capacity requirements, you will not be charged for that Spot

Instance. Unless you designate your Spot Instance Request as a persistent request, terminated Spot Instances will not automatically restart. You should save your work frequently and test your application to ensure it is fault tolerant and will correctly handle interruptions. We have no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from our termination of any Spot Instance. Spot Instances may not be used with certain Services, features and third-party software we specify, including Amazon DevPay, IBM software packages, or Microsoft SQL Server. You may not, directly, indirectly, alone or in cooperation with any third party, attempt to control, influence or manipulate the price for Spot Instances. Without limiting the foregoing, you may not submit requests for Spot Instances through any third party (e.g., “proxy bidding”) or share information with any third party regarding the maximum prices specified in your Spot Instance Requests. We may modify or terminate the Spot Instance Pricing program at any time. In addition to the Spot Instance Pricing, Spot Instances are subject to all data transfer and other usage fees applicable under the Agreement.

4.6. EC2 Reserved Instance Pricing. You may designate Amazon EC2 instances as subject to the reserved pricing and payment terms (“EC2 Reserved Instance Pricing”) set forth on the Amazon EC2 detail page on the AWS Site (each designated instance, a “EC2 Reserved Instance”). Scheduled EC2 Reserved Instances (“Scheduled Instances”) will terminate upon completion of the scheduled reservation. You may designate instances as EC2 Reserved Instances by calling to the Purchasing API or selecting the EC2 Reserved Instance option in the AWS console. When you designate instances as Reserved Instances, you must designate an availability zone, instance type, EC2 Reserved Instance type, and quantity for the applicable EC2 Reserved Instances. The EC2 Reserved Instances may only be used in the designated availability zone. We may change EC2 Reserved Instance Pricing at any time but price changes will not apply to previously designated EC2 Reserved Instances, except as described in this Section 4.6. If Microsoft increases the license fees it charges for Windows, or if Red Hat increases the license fees it charges for Red Hat Enterprise Linux (“RHEL”), we may make a corresponding increase to the per-hour usage rate (or institute a corresponding per-hour usage rate) for EC2 Reserved Instances with Windows or RHEL. Any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with Windows will be made between December 1 and January 31, and we will provide 30 days’ notice. For any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with RHEL we will provide 30 days’ notice. If this happens, you may: (a) continue to use your EC2 Reserved Instances with Windows or RHEL with the new per-hour usage price; (b) convert your EC2 Reserved Instances with Windows or RHEL to comparable EC2 Reserved Instances with Linux; or (c) terminate your EC2 Reserved Instances with Windows or RHEL and receive a pro rata refund of the up-front fee you paid for the terminated EC2 Reserved Instances with Windows or RHEL. We may terminate the EC2 Reserved Instance Pricing program at any time. EC2 Reserved Instances are nontransferable, except in accordance with the requirements of the RI Marketplace, but Scheduled Instances are not eligible for the RI Marketplace. EC2 Reserved Instances are noncancellable and you will owe the EC2 Reserved Instance Pricing for the duration of the term you selected, even if the Agreement is terminated.

All amounts paid in connection with the EC2 Reserved Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Reserved Instance type, or terminate the EC2 Reserved Instance Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated EC2 Reserved Instances. You may not purchase EC2 Reserved Instances for the purpose of reselling them in the RI Marketplace, and we reserve the right to refuse or cancel your purchase if we suspect you are doing so. Upon expiration or termination of the term of EC2 Reserved Instances, the EC2 Reserved Instance pricing will expire and standard on-demand usage prices will apply to the instances. In addition to being subject to EC2 Reserved Instance Pricing, EC2 Reserved Instances are subject to all data transfer and other fees applicable under the Agreement.

4.7 EC2 Reserved Instance (RI) Marketplace.

4.7.1. Eligibility. The rights to an active EC2 Reserved Instance can be offered for sale through the RI Marketplace as long as (1) the remaining term on the Reserved Instance is greater than one month, and (2) your payment of the upfront charge for it has been received and processed (for credit card purchases, 30 days after you have paid the upfront fee, and for invoice purchases, after you have paid the applicable invoice) (a “Marketable EC2 Reserved Instance”). The characteristics of the Marketable EC2 Reserved Instance (e.g., Instance Type, Platform, Region, Availability Zone, Tenancy, Hypervisor, Reserved Instance Type, Duration, and Hourly Price) will remain as originally designated. The term for the Marketable EC2 Reserved Instance will be the remainder of the original EC2 Reserved Instance term rounded down to the nearest month (for example, an EC2 Reserved Instance with 9 months and 16 days until expiration will be listed and sold as a 9 month Marketable EC2 Reserved Instance). You can be a “Seller” if you are a current AWS customer in good standing, you have a Marketable EC2 Reserved Instance associated with your AWS account, and you complete the registration process through your AWS account. Non-U.S.-based entities may not be Sellers without providing the Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) to establish that you are not a U.S. person. You can be a “Buyer” if you are a current AWS customer in good standing. You can resell an EC2 Reserved Instance that you previously purchased through the RI Marketplace. You may not resell an EC2 Reserved Instance that you purchased through a discount program (Reserved Instance Volume Discounts or otherwise) without obtaining our prior approval.

4.7.2. Submitting Marketable EC2 Reserved Instance for Sale. As a Seller, you will set the one-time price for your Marketable EC2 Reserved Instance. The hourly price will be the then-current hourly price for that type of EC2 Reserved Instance, and you will not receive any funds collected from payments associated with the hourly prices. You will pay the then-current fee to us specified on the AWS Site when your Marketable EC2 Reserved Instance is sold. Your Marketable EC2 Reserved Instance will be available for sale after you list it in the RI Marketplace, but it will remain yours and you will be able to use it until it is sold. You may remove a listing of Marketable EC2 Reserved Instance from the RI Marketplace at any time before it has been purchased by a Buyer. We may remove Marketable EC2 Reserved Instance from the RI Marketplace at any time for any

reason. Once sold and transferred to a Buyer, a Seller will have no rights to that Marketable EC2 Reserved Instance.

4.7.3. Our Role. As a Seller, you will be the seller of record of your rights to a Marketable EC2 Reserved Instance. Except as expressly set forth in these Service Terms, we are not involved in any underlying transaction between you and any Buyer. We or our affiliates may also participate in the market as a Seller or a Buyer.

4.7.4. Processing of Transactions; Collection of Transaction Proceeds. On Seller's behalf, we will process all payments for Transactions and collect the applicable Transaction Proceeds. "Transaction" means any sale of Marketable EC2 Reserved Instance through the RI Marketplace. "Transaction Proceeds" means the gross sales proceeds received by us from any Transaction. You will ensure that all fees and charges payable by Buyers for Marketable EC2 Reserved Instance are billed and collected through us and you will not offer or establish any alternative means of payment. We may impose transaction limits on some or all Buyers and Sellers relating to the value of any Transaction or disbursement, the cumulative value of all Transactions or disbursements during a period of time, or the number of Transactions that we will process over a period of time. We may withhold for investigation, or refuse to process, any of your Transactions that we suspect is fraudulent, unlawful or otherwise violates the terms of these Service Terms, the Agreement, or our Acceptable Use Policy. For each Transaction, we will not remit Transaction Proceeds to a Seller, and the Marketable EC2 Reserved Instance will be available to the Buyer, until after we have successfully processed payments for that Transaction from the Buyer.

4.7.5. Remittance of Transaction Proceeds to Sellers. At the end of each business day, we will pay to you all due and payable Transaction Proceeds that we have collected as of the date that is 2 business days prior to the date of payment. We will deduct from each payment any applicable fees and charges due to us related to Marketable EC2 Reserved Instances. The applicable fees and charges are posted on the AWS Site and may be changed from time to time. We may withhold, deduct, or setoff any amounts payable by you to us or our affiliates against any Transaction Proceeds. Payments will be made only to an ACH-enabled bank account located in the United States that you register with us. If there is an error in the processing of any Transaction, you authorize us to initiate debit or credit entries to your designated bank account, to correct such error, provided that any such correction is made in accordance with applicable laws and regulations. If we are unable to debit your designated bank account for any reason, you authorize us to resubmit the debit, plus any applicable fees, to any other bank account or payment instrument that you have on file with us or to deduct the debit and applicable fees from future Transaction Proceeds.

4.7.6. Taxes. Sellers are responsible for the calculation, validation and payment of any and all sales, use, excise, import, export, value added, withholding and other taxes and duties assessed, incurred or required to be collected ("Taxes") or paid for any reason in connection with any Transaction and with Marketable EC2 Reserved Instance. We are not obliged to determine whether any Taxes apply to any Transaction, and we are not responsible for remitting Taxes to any taxing authority with respect to any Transaction, or for reporting any information (including the payment of Taxes) with respect to any

Transaction. Each Seller will indemnify us and our affiliates against any claim or demand for payment of any Taxes imposed in connection with any Transaction, and for any fines, penalties, or similar charges imposed as a result of the Seller's failure to collect, remit or report any Taxes in connection with any Transaction.

4.7.7. Data Collection and Sharing. For each Seller, we will collect the necessary data and tax forms to enable compliance with applicable tax laws. For example, for U.S.-based Sellers, we will collect and retain Seller name and address, and may collect the tax identification number and other data as needed to comply with Form 1099K reporting requirements; for non-U.S.-based Sellers, we will collect and retain a Form W-8BEN tax form (which includes name, address, and a signature) as proof that you are exempt from Form 1099K reporting. For each Buyer, we will collect and retain the Buyer's name and address. Buyers and Sellers will not know the name of the other party to the Transaction until the Transaction is completed. Upon completion of the Transaction, we will share the applicable Buyer's city, state, and zip with the Seller so that the Seller can calculate the appropriate tax (if any) to remit to the appropriate government entity. We will share the Seller's legal name on the Buyer's invoice. Buyers and Sellers may not use information about the Transaction or about the other party gained in connection with a Transaction ("Transaction Information") for any purpose that is not related to the Transaction. For example, you may not, directly or indirectly: (1) disclose any Transaction Information to any third party, except as necessary for you to perform your tax obligations or other obligations under these Service Terms and only if you ensure that every recipient uses the information only for that purpose and complies with these restrictions; (2) use any Transaction Information for any marketing or promotional purposes whatsoever; (3) use any Transaction Information in any way inconsistent with applicable law; (4) contact a party to influence them to make an alternative sale or purchase; (5) disparage us, our affiliates or any of their or our respective products; or (6) target communications of any kind on the basis of the intended recipient being an RI Marketplace Buyer or Seller.

4.8 You may only use the AWS Management Pack for System Center on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Management Pack for System Center is governed by the license agreement, located here: AWS Management Pack for System Center License Agreement<http://aws.amazon.com/windows/system-center/aws-mp-license>.

4.9 Dedicated Instances. You may request that certain Amazon EC2 instances run on physically isolated host hardware dedicated to a single customer account (each requested instance, a "Dedicated Instance"), using the process set forth on the Amazon EC2 Dedicated Instance detail page on the AWS Site.

4.10 Dedicated Hosts.

4.10.1 You may request that Amazon provide the Amazon EC2 service to you on host hardware physically dedicated to a single customer account (each, a "Dedicated Host"), using the process set forth on the AWS Site.

4.10.2 You may designate Amazon EC2 Dedicated Hosts as subject to the reservation pricing and payment terms (“EC2 Dedicated Host Reservation Pricing”) set forth on the Amazon EC2 detail page on the AWS Site (each such host associated with a reservation, an “EC2 Dedicated Host Reservation”). You may associate EC2 Dedicated Host Reservations to Dedicated Hosts by calling APIs or using the EC2 Dedicated Host Reservation console. The EC2 Dedicated Host and associated EC2 Dedicated Host Reservation may only be used in the designated availability zone. We may change EC2 Dedicated Host Reservation Pricing at any time but price changes will not apply to previously designated EC2 Dedicated Host Reservations, except as described in this Section 4.10.2. We may terminate the EC2 Dedicated Host Reservation Pricing program at any time. EC2 Dedicated Host Reservations are nontransferable. EC2 Dedicated Host Reservations are noncancellable and you will owe the EC2 Dedicated Host Reservation Pricing for the duration of the term you selected, even if the Agreement is terminated. Dedicated Hosts associated to an active EC2 Dedicated Host Reservation cannot be unallocated from your account, and you will continue to pay for the Dedicated Host while still associated with the EC2 Dedicated Host Reservation. All amounts paid in connection with the EC2 Dedicated Host Reservations are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Dedicated Host type, or terminate the EC2 Dedicated Host Reservation Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated EC2 Dedicated Host Reservation. Upon expiration or termination of the term of an EC2 Dedicated Host Reservation, the EC2 Dedicated Host Reservation Pricing will expire and standard on-demand Dedicated Host prices will apply to the Dedicated Host. In addition to being subject to EC2 Dedicated Host Reservation Pricing, EC2 Dedicated Host Reservations are subject to all data transfer and other fees applicable under the Agreement.

4.11 Microsoft BYOL Licensing. Under this option, Amazon EC2 enables you to provision Amazon EC2 instances using your Microsoft Software and Microsoft Licenses (the “BYOL Program”). Unless otherwise specified in your agreement(s) with Microsoft, you can use this benefit only if you comply with the requirements [here](#) , and you (a) use Dedicated Instances or Dedicated Hosts; (b) launch from Virtual Machines (VMs) sourced from software binaries provided by you; and (c) run the instances within your designated AWS regions.

You must be eligible to use the BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using the Microsoft Software under the BYOL Program, you agree to the Microsoft EULA.

You agree that you have determined that your use of the BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted.

4.12 As part of using Amazon EC2, you agree that your Amazon EC2 resources may be terminated or replaced due to failure, retirement or other AWS requirement(s). We have

no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from the foregoing. THE USE OF AMAZON EC2 DOES NOT GRANT YOU, AND YOU HEREBY WAIVE, ANY RIGHT OF PHYSICAL ACCESS TO, OR PHYSICAL POSSESSION OF, ANY AWS SERVERS, EQUIPMENT, REAL OR PERSONAL PROPERTY, OR OTHER ASSETS.

5. Alexa® Web Services

5.1. You may use Alexa® Web Services to create or enhance applications or websites, to create search websites or search services, to retrieve information about websites, and to research or analyze data about the traffic and structure of the web.

5.2. You may not display data you receive via the Alexa® Services that has been cached for more than 24 hours.

5.3. You may not resell or redistribute the Alexa® Web Services or data you access via the Alexa® Web Services.

5.4. You may use data you receive from the Alexa® Web Services, such as web site traffic data, to enhance your application or website, but may not use it in any application whose primary purpose is to display the same or related data or whose primary purpose is to compete with www.alexacom .

6. Amazon Flexible Payments Service (Amazon FPS)

6.1. The terms in this Section 6 apply only to Amazon FPS and use of Your Content with the web-based payment service provided by Amazon Payments, Inc. (“Amazon Payments”) that enables the processing of payment transactions initiated by third parties, and that may include, without limitation, the processing and settlement of credit card transactions, bank transfers, or the administration of prepaid or post-paid balances (the “Payment Service”).

6.2. You may:

- access and use Amazon FPS to enable use of the Payment Service by users who have an appropriate Payment Service account (each, an “Amazon Payments User”) via Your Content in accordance with any applicable FPS Specifications (as defined below);
- install, copy, and use the software development kit provided by us as part of Amazon FPS, including the related development guides and technical documentation (collectively, the “FPS SDK”), and access and use the online testing environment made available by us (the “FPS Sandbox”), in each case as necessary to internally develop and test Your Content for use with the Payment Service; and
- create, incorporate, compile, and copy derivative works of the sample computer programming code provided by us for development and testing of Your Content (the “FPS Sample Code”) as part of Your Content for distribution in machine readable binary form or object code form to Amazon Payments Users as necessary for them to

use the Payment Service. Use of FPS Sample Code is also subject to any additional license terms included with the FPS Sample Code. Such additional terms will control in the event of any inconsistency or conflict with the Agreement.

6.3. The FPS SDK, FPS Sample Code, and FPS Specifications (as defined below) constitute Amazon Properties. Except as expressly authorized by this Section 6, you may not sublicense, loan, sell, assign, lease, rent, transfer, act as a service bureau, distribute or grant rights to any person or entity in Amazon FPS, the FPS SDK, the FPS Sandbox or the Payment Services.

6.4. You and Your Content will comply with any technical and operational specifications and other documentation or policies provided or made available by us or Amazon Payments with respect to Amazon FPS or the Payment Service respectively (the “FPS Specifications”). We reserve the right to update or modify the FPS Specifications at any time. Prior to making Your Content generally available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FPS, including without limitation that it complies with the FPS Specifications.

6.5. We may review and test Your Content to confirm that it operates properly with Amazon FPS and complies with the FPS Specifications, using review and test processes determined in our sole discretion. You agree to correct any material errors, defects or other non-compliance of which you become aware, including from review and test results provided by us. We may make modifications, updates or upgrades to Amazon FPS, the FPS SDK, or FPS Specifications. In such event, you will test and, if necessary, modify Your Content to ensure that it continues to operate properly with the then-current version of Amazon FPS, the FPS SDK, and FPS Specifications.

6.6. You must establish and maintain a payments account with Amazon Payments to use Your Content commercially with Amazon FPS and to access the Payment Service. Your use of the Payment Service is subject to Amazon Payment’s policies, procedures, and user agreements, and any breach of the foregoing will constitute a breach of the Agreement. In addition to the limitations described in the Agreement, any use of the Amazon Payments logo and trademark is subject to the trademark usage guidelines issued by Amazon Payments.

6.7. You are responsible for (a) the collection and payment of any and all sales, use, excise, import, export, value added and other taxes and duties assessed, incurred or required to be collected or paid for any reason in connection with any offer or sale of products or services by you, including Your Content, and (b) any payment transaction that is initiated using Your Content that is charged back or reversed (a “Chargeback”) to the extent that such Chargeback is attributable to any error, act or omission of you or Your Content and is not otherwise recovered by Amazon Payments from an Amazon Payments User. You will indemnify and reimburse Amazon Payments and its affiliates against any claim or demand for payment of any such taxes or any Chargebacks.

6.8. You represent, warrant, and covenant that you will at all times:

- represent the capabilities and features of the Payment Service consistent with our description of such capabilities and features and avoid false, deceptive, misleading or

unethical practices that may be detrimental to us or Amazon Payments, the Payment Service, Amazon Payments Users or other third parties;

- refrain from providing warranties or disclaimers with respect to the Payment Service;
- promptly investigate and report to us all complaints received by you with regard to Amazon FPS and the Payment Service, and make every reasonable effort to maintain and promote good public relations for us in the handling of any such complaints; and
- ensure that the terms of any agreements between you and any Amazon Payments User are consistent with the terms of the Agreement and these Service Terms.

7. Amazon DevPay Service (Amazon DevPay)

7.1. You may use Amazon DevPay to: (a) sell to end users (“Customers”) use of Your Content that you develop and make available with the Services (the “Bundled Application”), including machine images that you develop; (b) establish accounts for Customers that use the Bundled Application (“Customer Accounts”); (c) manage features of Customer Accounts; and (d) receive payments from Customers for Bundled Applications.

7.2. You will establish the pricing applicable to Customers for their use of any Bundled Application. We will only be responsible for collecting those fees that are fully disclosed and properly configured within the DevPay Service. The fees you charge to Customers for your Bundled Applications through the DevPay Service (as further described in Section 7.6 below) must constitute the full and complete fees you charge Customers for such Bundled Applications. You may not charge or impose any additional or supplemental fees for Bundled Applications other than those disclosed through the DevPay Service. While you are using the DevPay Service, you shall not establish any alternative means of payment for such Bundled Applications. The foregoing does not limit your ability to charge and receive payments for goods and services other than the Bundled Application sold through the DevPay Service.

7.3. You are responsible for designating all terms and conditions applicable to the use of the Bundled Application; provided that, use of the underlying Services are subject to the terms of the Agreement which will control in the event of a conflict. We may require users to register an AWS account (including agreeing to the terms of the Agreement) in order to use Amazon EC2 or other Services associated with the Bundled Application. You may not extend on behalf of us any written or oral warranty or guarantee, or make any representation or claim, with respect to the Services without our prior written consent. Upon termination of the Agreement or the [Amazon Payments, Inc. Customer Agreement](#) for any reason, all access by Customers with respect to your Bundled Applications may be terminated by us.

7.4. Except as set forth in Section 7.5 below, you are fully liable for all charges incurred for Services under your account identifiers or those assigned to your Customers for your Bundled Applications. All Services will be charged at the then current price applicable to such Services under the Agreement. Payments will be processed by Amazon

Payments, Inc. and are subject to the terms of the [Amazon Payments, Inc. Customer Agreement](#) , including your liability for chargebacks. All payments collected using the DevPay Service are subject to the then current processing fee described on the DevPay detail page on the AWS Site. Amounts owed under the Agreement may be deducted from proceeds collected under the [Amazon Payments, Inc. Customer Agreement](#) .

7.5. If we are unable to collect the fees you specify from your Customers for the sale of your Bundled Applications (“Customer Fees”) or a prior transaction for those fees is reversed, you will not be responsible for paying the fees for the Services used by you and your Customer (“Service Fees”) and AWS will have no obligation to remit or otherwise seek collection of the Customer Fees, provided that the payment failure is due to:

- AWS’s inability to charge a Customer’s credit card for the Customer Fees, or
- A transaction is reversed as a result of a Chargeback (as described in the [Amazon Payments, Inc. Customer Agreement](#)) because the transaction was not authorized or was otherwise fraudulent.

In addition, in the applicable month, the Customer Fees charged must exceed the Service Fees. In the event of such a payment failure, we may recover or otherwise set off any Customer Fees from you that we collected in the month to the extent they do not exceed the Service Fees. In the event that either you or AWS is subsequently able to collect the Customer Fees, you will pay to AWS the corresponding Service Fees as provided in the Agreement.

7.6. We will host and make available to Customers a customer interface (“Customer UI”) permitting (a) the display to Customers of certain pricing, terms and conditions and other information you provide to us regarding your Bundled Applications (“Subscription Information”) and (b) Customers to engage in certain functions with respect to your Bundled Applications, such as account establishment, account termination, payment authorization and termination rights. We will define and control the fields and format for the Customer UI and for Subscription Information. We retain all rights to the Customer UI, including its look and feel, and you will not copy or mimic the Customer UI in any manner.

7.7. You are responsible for ensuring and shall ensure that all Subscription Information (as you provide it to us and as it is ultimately shown on the Customer UI) is: (a) full, accurate and complete, (b) not misleading; and (c) in compliance, in all respects, with applicable laws. You must promptly update the Subscription Information when and as necessary to ensure that the Subscription Information continues to comply with the foregoing requirements, even if the updates are necessary as a result of changes we make to the data input fields or to the Customer UI.

7.8. You are responsible for providing customer service (if any) to Customers for your Bundled Applications. We shall have no obligation to provide customer or technical support to any Customer for Bundled Applications; provided that, we will provide support to Customers regarding billing and payment questions.

7.9. You will use the communication methods we establish through the DevPay Services for the administration of Customer Accounts, including, but not limited to, any communications regarding Customer Account termination or pricing changes.

7.10. You acknowledge and agree that we may take any of the corrective action regarding Customer Accounts to the extent we deem necessary or appropriate, in our sole discretion, to (a) comply with law, (b) enforce or apply the Agreement, the [Amazon Payments, Inc. Customer Agreement](#), or other agreements or policies applicable to the Services or DevPay Service, or (3) protect the rights, property or safety of our business, a Customer, or any third party. Corrective action may include (i) suspending, canceling or closing of Customer Accounts; (ii) re-establishment of Customer Accounts; and (iii) waiving or refunding of fees on Customer Accounts. We shall have no liability to you for taking any such actions. You shall promptly comply with any actions we take or may require of you regarding Customer Accounts. These actions may include, without limitation, reimbursing us for Customer refunds we issue, discontinuing provision of services on Customer Accounts we cancel, and re-establishment of services on Customer Accounts we re-establish. Should you ask us to close a Customer Account by using a method we have provided for that purpose, we will endeavor to close the Customer Account reasonably promptly, but we shall have no liability to you for the speed with which we do so or for our failure to do so. You shall indemnify and hold us and our employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys fees), arising out of or in connection with any claim based on or related to any actions we may take with respect to any Customer Account at your direction, including, without limitation, any closure of a Customer Account.

7.11. You acknowledge and agree that: (a) you have no expectation and have received no assurances that your business relationship with us will continue beyond the Term (or its earlier termination), that any investment by you in the promotion of any Bundled Application will be recovered or recouped, or that you will obtain any anticipated amount of profits; and (b) you will not have or acquire by virtue of the DevPay Services or otherwise any vested, proprietary or other right in the promotion of any Services or in any related goodwill created by your efforts.

8. Amazon SimpleDB Service (Amazon SimpleDB)

8.1. If during the previous six (6) months you have incurred no fees for Amazon SimpleDB and have registered no usage of Your Content stored in Amazon SimpleDB, we may delete, without liability of any kind, Your Content that is stored in Simple DB upon thirty (30) days prior notice to you.

9. Amazon Fulfillment Web Service (Amazon FWS)

9.1. You may only access and use Amazon FWS to query, access, transmit and receive product and shipping information related to your use of the Fulfillment by Amazon service ("FBA Service") sold and provided by Amazon Services LLC ("Amazon Services") in accordance with any applicable FBA Specifications (as defined below).

9.2. To use Amazon FWS, you must have an Amazon seller account (your “Seller Account”) that is in good standing and be registered to use the FBA Service. Your use of the FBA Service and your Seller Account is solely subject to Amazon Services’ policies, procedures, the Amazon Business Services Agreement or other applicable user agreements. Amazon FWS is only a technical interface that enables you to access and process certain information related to your Seller Account. AWS will have no liability to you or any third party related to your Seller Account.

9.3. You may use Amazon FWS only to administer product and shipping information associated with your Seller Account. When registering for Amazon FWS, you must use the same username and password which is associated with your Seller Account. You may not develop or use an application to access Amazon FWS that collects, processes or stores the account identifiers or other security credentials (including usernames and passwords) of any third party associated with AWS or any of its affiliates.

9.4. You and Your Content will comply with any technical and operational specifications, security protocols and other documentation or policies provided or made available by us with respect to Amazon FWS (the “FBA Specifications”). We reserve the right to update or modify the FBA Specifications at any time. Prior to making Your Content available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FWS, including, without limitation, that it complies with the FBA Specifications.

10. Amazon Elastic MapReduce

10.1. We may collect certain information about computing jobs you run using Amazon Elastic MapReduce, including CPU utilization, memory usage, IO performance, and error and information messages.

10.2. You are responsible for all fees incurred from your use of Amazon Elastic MapReduce regardless of the results obtained, the quality of the resulting data, or whether a computing job runs successfully. Use of Amazon Elastic MapReduce requires use of Amazon EC2 and Amazon S3, and certain features require use of Amazon SimpleDB. You are responsible for the separate fees you accrue for Amazon EC2, Amazon S3, and Amazon SimpleDB.

10.3. You are solely responsible for monitoring the status of your computing jobs. We may throttle or terminate computing jobs that we determine degrade the performance of Amazon Elastic MapReduce, the Services, or any component of the Services. We are not responsible for any data loss or data corruption that occurs as part of your computing jobs.

11. Amazon CloudWatch and Auto Scaling

11.1. You may only use Amazon CloudWatch to perform monitoring and auto-scaling functions in connection with Amazon EC2. Amazon CloudWatch enables Auto Scaling in connection with Amazon EC2. Auto Scaling requires use of both Amazon CloudWatch and Amazon EC2.

11.2. In connection with Auto Scaling, we may launch additional Amazon EC2 instances or terminate Amazon EC2 instances based on conditions you set. You are responsible for the separate fees you accrue for Amazon EC2. You are responsible for all fees incurred from your use of Amazon CloudWatch and Auto Scaling regardless of the results obtained or the quality or timeliness of the results. Charges for Amazon CloudWatch will accrue as soon as you use begin using Amazon CloudWatch or Auto Scaling functionality.

11.3. Amazon CloudWatch collects and stores certain information for the Amazon EC2 instances you are monitoring, including CPU utilization, data transfer, and disk usage and activity. Amazon CloudWatch metric data is kept for 14 days; we may delete CloudWatch metric data, without liability of any kind, at any time after 14 days.

12. Elastic Load Balancing

12.1. You may only use Elastic Load Balancing to provide load balancing functionality in connection with Amazon EC2. You must have instances running in all Availability Zones across which you want to balance loads with Elastic Load Balancing.

12.2. Use of Elastic Load Balancing requires use of Amazon EC2. You are responsible for the separate fees you accrue for Amazon EC2. You are responsible for all fees incurred from your use of Elastic Load Balancing regardless of the results obtained or the quality or timeliness of the results. Charges for Elastic Load Balancing will accrue as soon as you use begin using Elastic Load Balancing functionality.

13. AWS Import/Export

13.1. As part of AWS Import/Export Disk, you may send physical storage media (the “Media”) to us that we will use to either (a) transfer data contained on the Media into supported AWS Services as Your Content or (b) transfer certain of Your Content to the Media (such data contained on Media either before or after transfer, “Data”) and provide the Media to you.

13.2. You will not deliver to us, and we may refuse to accept any, damaged, defective or unreadable Media or any Media otherwise not shipped in accordance with the Agreement (collectively, “Unsuitable Media”). We may return or dispose of any Unsuitable Media, or erase Data on such Unsuitable Media. In addition, you will reimburse us for any expenses we incur in connection with any Unsuitable Media. If you request and we return Unsuitable Media to you, you agree that we will select the shipping carrier and handling standards for return of such Unsuitable Media in our sole discretion, and the carrier and standards may not be the same (and may cost more) than those we use for shipping media in connection with AWS Import/Export generally. For avoidance of doubt “Media” includes “Unsuitable Media”.

13.3. As part of AWS Import/Export Snowball, we will ship you an agreed upon number of network-attached storage appliances (each an “Appliance”) and provide you with access to the AWS Snowball Client (together with the software contained on the Appliance, and any updates or upgrades to the foregoing, the “Software”). AWS Import/Export Snowball availability is limited to certain AWS regions and account types;

please contact us to see if you qualify. You agree that you will not allow any Appliance to leave the United States state or non-U.S. country to which the Appliance is shipped until you deliver it (in the same U.S. state or non-U.S. country) to a carrier for redelivery to us. After you receive an Appliance, you may transfer certain of Your Content onto the Appliance as “Data” and provide the Appliance to the carrier for return to us. Once we receive the Appliance, we will transfer the Data on the Appliance into a supported AWS Service as Your Content.

13.4. You will comply with all specifications and documentation for AWS Import/Export as provided and updated by us from time to time, including shipping and encryption requirements, the [AWS Import/Export Disk Pack and Ship Check List](#), the AWS Import/Export Snowball User Guide, and any documentation on the AWS Site or an Appliance.

13.5. You will be solely responsible for all shipping and handling costs (which may include costs of freight and transit insurance) for shipping Media and Appliances to or from us. For AWS Import/Export Disk, we may pay some reasonable return shipping charges as described on the AWS Import/Export Disk section of the AWS Site. You are responsible for payment of all customs, duties, taxes and other charges in connection with Media and Appliances being shipped to or from us. Use of AWS Import/Export requires use of a supported AWS Service. You are responsible for the separate fees you accrue for AWS Services.

13.6. We have no liability or responsibility with respect to any delay, damage or loss incurred during shipment in connection with AWS Import/Export, including loss of Data. For AWS Import/Export Disk, you will bear the entire risk of loss of, or damage to, any Media (including Data) while in transit and you are solely responsible for obtaining insurance at your expense. For AWS Import/Export Snowball, you are responsible for the entire risk of loss of, or any damage to, an Appliance once it has been delivered by the carrier to your address until the carrier accepts the Appliance for delivery back to Amazon. If you have not provided an Appliance to the carrier for delivery to Amazon for any reason within 12 days of the date it was delivered to your address, we may charge you a late fee as described on the AWS Import/Export Snowball section of the AWS Site. If you have not provided an Appliance to the carrier for return to Amazon within 90 days of the date it was delivered to you, we may charge you a lost device fee of \$7500, in addition to the applicable late fees. If we receive an Appliance back from you and it has any damage which it did not have when we sent it to you, you may be charged the cost to us of fixing the damage or, if the damage cannot be reasonably fixed, the lost device fee described in the previous sentence.

13.7. You will retain title to any Media and Data we receive from you and store on an AWS Service as part of AWS Import/Export. You supply us with Media and Data entirely at your own risk. You should back-up Data prior to transfer onto an Appliance or Media and prior to delivery to us. Your Data should not include live or production data or any other data that you are not prepared to lose. We are not responsible for and will not be held liable for any damage to Media or any loss of Data. Our confirmed receipt of delivery does not: (a) indicate or imply that any Media, Appliance or Data has been delivered free of loss or damage, or that any loss or damage to any Media, Appliance or

Data later discovered occurred after confirmed receipt of delivery; (b) indicate or imply that we actually received the number of units of Media specified by you for such shipment; or (c) waive, limit or reduce any of our rights under the Agreement. We reserve the right to impose, and change, from time to time, volume limitations on the delivery of your Media, and you will comply with any of these restrictions or limitations.

13.8. You represent that you have all necessary rights to (a) provide the Media and Data to us for upload into supported AWS Services and (b) authorize our transfer of any Data specified by you to the Media. You represent that import or export of the Media or Data to or from us does not require a license under the laws or regulations of any country. We may reproduce Data as necessary to transfer it between Media or Appliances and supported AWS Services.

13.9. IN ADDITION TO THE DISCLAIMERS IN THE AGREEMENT, WE HEREBY DISCLAIM ANY DUTIES OF A BAILEE OR WAREHOUSEMAN, AND YOU HEREBY WAIVE ALL RIGHTS AND REMEDIES OF A BAILOR (WHETHER ARISING UNDER COMMON LAW OR STATUTE), RELATED TO OR ARISING OUT OF ANY POSSESSION, STORAGE OR SHIPMENT OF MEDIA OR DATA BY US OR OUR AFFILIATES OR ANY OF OUR OR THEIR CONTRACTORS OR AGENTS. YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA. You use the Appliances and Software entirely at your own risk. We are not responsible and will not be liable for any damage to, or any loss or misuse of, systems or equipment you use in connection with the Appliances and Software.

13.10. In addition to your indemnification obligations under the Agreement, you agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys' fees), arising out of or in connection with any claim arising out of (a) the Media (whether or not title has transferred to us) and Data, including any personal injury, death or property damage (including any damage caused by malicious or harmful code included in Data); (b) any sales, goods and services, use, excise, import, export, property, value added or other taxes or duties assessed or imposed on us or our affiliates in connection with or as a result of the storage, shipping or other actions taken by you with respect to the Appliances or taken by us with respect to the Media or Data; (c) any legal or regulatory violation, arising under the laws or regulations of any country, related to import or export of the Media or the Data.

13.11. Once AWS Import/Export services are complete, we will return the Media to you (for AWS Import/Export Disk) or delete the Data from the Appliance (for AWS Import/Export Snowball). We may return Media to you for any reason, including upon termination of the Agreement or the AWS Import/Export service. Returned Media will be sent to your designated shipping address. Media shipped to us for import into or export from supported AWS Services in the EU (Ireland) Region must originate from and be returned to an address within the European Union. If we have an outdated, incorrect or

prohibited address for you, we will attempt to notify you and you will have thirty (30) calendar days from the date we provide notification to supply a substitute address. If you do not supply a substitute address within thirty (30) calendar days of notification, the Media will be deemed Unsuitable Media subject to disposal. We may erase Data and dispose of Media in any manner and we have no obligation to reimburse or compensate you for any loss of Media or Data due to our disposal.

13.12. Notwithstanding anything to the contrary in the Agreement, you may give agents and subcontractors of your choosing access to the private key associated with your AWS account solely for the purpose of (a) preparing Data for import or export using AWS Import/Export or (b) confirming the integrity of Data imported or exported using AWS Import/Export. You remain fully responsible for and indemnify us for all activities undertaken by such third parties under your account. Other than as specifically set forth in this section, all terms and conditions of the Agreement continues to apply to your use of the Services.

13.13. The Appliances, the Software and all other proprietary information, know-how, programming, software, trademarks, trade secrets, plan drawings, requirements, specifications, designs, and patterns furnished or created by us or our agents or contractors and all property rights embodied therein are and will remain our sole property at all times. At no point do we sell, rent, lease or transfer any ownership or other rights to the Appliance to you. You may not use the Appliance in any manner not expressly permitted herein. Without limiting the foregoing, you will not, and will not permit or authorize third parties to (or attempt to), (a) disassemble or reverse engineer the Appliance or the Software; (b) open, modify, alter or otherwise tamper with the Appliance; (c) circumvent or disable any features or measures in the Appliance or the Software. Your use of the Software is governed by the licenses included with the Software. Certain components of the Software included on Appliances are governed by the open source software licenses identified [here](#) . Your license rights with respect to such components are defined by the applicable open source software license.

13.14. For AWS Import/Export, Disk, we will not act as the importer of record for your shipments of Media or Data. If we are importing or exporting your shipments of Media or Data into the Asia Pacific (Singapore) Region, you will not act as the importer of record and you represent and warrant that: (a) You are not a resident of Singapore; (b) You have a business establishment or fixed establishment outside of Singapore and not in Singapore; (c) You are domiciled outside Singapore if you have no business or fixed establishment in any country; (d) You are not registered or required to be registered for GST in Singapore.

You will notify us if, at any time, you are using the AWS Import/Export Disk service to ship Media or Data into the Asia Pacific (Singapore) Region and you are not acting as the importer of record, and you become unable to make any of the above representations and warranties.

If you are not acting as the importer of record on your shipment of Media or Data to the Asia Pacific (Singapore) Region, then the Media or Data must (i) be returned to a

location outside of Singapore, (ii) be exported on an FCA basis; and (iii) you must be importer of record in the country that the Media or Data is returned to.

14. Amazon Virtual Private Cloud (Amazon VPC)

14.1. You may only use Amazon VPC to connect your computing resources to certain AWS computing resources via a Virtual Private Network (VPN) connection.

14.2. Use of Amazon VPC requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with Amazon VPC. When you transfer data between AWS computing resources running inside Amazon VPC and AWS computing resources running outside Amazon VPC, you will be charged VPN data transfer rates in addition to any applicable Internet data transfer charges. VPN connection charges accrue during any time your VPN connection is in the “available” state.

14.3. You are solely responsible for the configuration, operation, performance and security of all equipment and computing resources you use with Amazon VPC, including any gateways or other devices you use to connect to Amazon VPC.

15. AWS Multi-Factor Authentication (AWS MFA)

15.1. You may only use AWS MFA in connection with accessing your AWS account.

15.2. Your use of AWS MFA requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with AWS MFA.

15.3. You are solely responsible for the procurement and for the configuration, operation, performance and security of any hardware or non-AWS software that you use in connection with AWS MFA, including any compatible authentication devices.

16. Amazon Relational Database Service (Amazon RDS)

16.1. You may only use Amazon RDS to store, query, retrieve and serve data and other content owned, licensed or lawfully obtained by you. You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for the proper configuration of database security groups and other security settings associated with Amazon RDS.

16.2. You may store snapshots of Your Amazon RDS Content for later use in Amazon RDS but snapshots cannot be downloaded outside the Services.

16.3. We may terminate your Amazon RDS database instance if you attempt to access or tamper with any software we pre-load on the database instance, including the operating system software running on the database instance.

16.4. You are responsible for configuring your backup retention period to give yourself enough time to recover data from your backups in the event of a hardware or file system failure.

16.5. Reserved DB Instance Pricing. You may designate Amazon RDS database instances as subject to the reserved pricing and payment terms (“Reserved DB Instance Pricing”) set forth on the Amazon RDS detail page on the AWS Site (each designated instance, a “Reserved DB Instance”). You may designate database instances as Reserved DB Instance by calling to the Purchasing API or selecting the Reserved DB Instance option in the AWS console. When you designate a database instance as a Reserved DB Instance, you must designate a region, instance type and quantity for the applicable Reserved DB Instances. The Reserved DB Instances may only be used in the designated region. We may change Reserved DB Instance Pricing at any time but price changes will not apply to previously designated Reserved DB Instances. We may terminate the Reserved DB Instance Pricing program at any time. Reserved DB Instances are noncancellable, and you will owe the Reserved DB Instance Pricing for the duration of the term you selected, even if the Agreement is terminated. Reserved DB Instances are nontransferable and all amounts paid in connection with the Reserved DB Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved DB Instance type, or terminate the Reserved DB Instance Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved DB Instances. Upon expiration or termination of the term of a Reserved DB Instance, the Reserved DB Instance Pricing will expire and standard on-demand usage prices will apply to the database instance. In addition to being subject to Reserved DB Instance Pricing, Reserved DB Instances are subject to all data transfer and other fees applicable under the Agreement.

16.6. Using Oracle Software.

16.6.1 “License Included”. As part of the Services, you may be allowed to use certain software (including related documentation) described on the AWS Site developed and owned by Oracle America, Inc. or its affiliates (“Oracle”) and Oracle’s licensors (collectively, the “Oracle Software”). If you choose to use the Oracle Software and do not already have a license from Oracle for that Oracle Software, Oracle and its licensors require that you agree to these additional terms and conditions:

- Oracle or its licensors retains all ownership and intellectual property rights in the Oracle Software, and title to the Oracle Software does not transfer to you or any third party by virtue of this Agreement.
- The Oracle Software is subject to a restricted license and may only be used in connection with the Service Offerings, and only by the individual or legal entity that entered into the Agreement.
- You may only use the Oracle Software for your internal business operations and in accordance with the Agreement. You may permit agents or contractors (including outsourcers) to use the Oracle Software on your behalf for the purposes set forth in, and subject to, the Agreement, provided you are responsible for the agent’s, contractor’s and outsourcer’s compliance with the Agreement in connection with such use.

- You may not:
 - assign, grant, or transfer the Oracle Software or any interest in the Oracle Software to another individual or entity, and if you purport to grant a security interest in the Oracle Software, the secured party will have no right to use or transfer the Oracle Software;
 - use the Oracle Software for rental, timesharing, subscription services, hosting, or outsourcing;
 - remove or modify any notice of Oracle's or its licensors' proprietary rights;
 - make the Oracle Software available in any manner to any third party for use in the third party's business operations;
 - duplicate, reverse engineer (unless required by law for interoperability), disassemble or decompile the Oracle Software (including by reviewing data structures or similar materials produced by the Oracle Software); or
 - publish any results of benchmark tests run on the Oracle Software.
- Third party technology that may be appropriate or necessary for use with some Oracle Software is specified in the related documentation, and that third party technology is licensed to you only for use with the Service Offerings and under the terms of the third party license agreement specified in the documentation, not this Agreement.
- To the extent permitted by applicable law, Oracle disclaims any liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from your use of the Oracle Software.
- Notwithstanding anything to the contrary elsewhere in the Agreement, Oracle is an intended third party beneficiary of the Agreement, but solely with respect to this Section 16.6.1 of these Service Terms.
- The Uniform Computer Information Transactions Act does not apply to your use of the Oracle Software.
- Upon any termination of the Agreement, you must discontinue use of the Oracle Software and any related documentation.

16.6.2 "Bring-Your-Own-License" (BYOL). Under the BYOL option, Amazon RDS enable you to provision Oracle Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the Oracle Software. You can use the Oracle Software with Amazon RDS if you meet the following conditions:

- You must have a valid license with "Software Update License & Support" for the Oracle Software you wish to run. The terms of your existing license and support agreement(s) with Oracle continue to apply to your use of the Oracle Software; and

- You must follow Oracle's current policies for licensing Oracle Database software in the cloud computing environment. The database instances using the Oracle Software with Amazon RDS reside in the Amazon EC2 environment.

16.7 Using Microsoft Software.

16.7.1 "License Included." In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the "Microsoft Software"). If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, "High Risk Use"). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- SQL Server Web Edition may be used only to support public and Internet accessible Web pages, Web sites, Web applications or Web services. It may not be used to support line of business applications (e.g., Customer Relationship Management, Enterprise Resource Management and other similar applications).

16.7.2 License Mobility with Software Assurance (Bring Your Own License or BYOL). Under this option, Amazon RDS enable you to provision Microsoft SQL Server

Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the SQL Server Software. You can use this benefit if only you meet the requirements and have signed up as described [here](#).

16.7.3 Microsoft is an intended third-party beneficiary of this Section 16.7, with the right to enforce its provisions.

17. Amazon Simple Notification Service (Amazon SNS)

17.1. You may only use Amazon SNS to send notifications to parties who have agreed to receive notifications from you.

17.2. We may throttle or restrict notifications if we determine, in our sole discretion, that your activity may be in violation of the AWS Acceptable Use Policy or the Agreement.

17.3. Your notifications sent through Amazon SNS may be blocked, delayed or prevented from being delivered by destination servers and other reasons outside of our control and there is no warranty that the service or content will be uninterrupted, secure or error free or that notifications will reach their intended destination during any stated time-frame. In addition, you acknowledge that we may not be able to provide the service if a wireless carrier delivering Amazon SNS notifications by short messaging service (SMS) terminates or suspends their service. Your payment obligations may continue regardless of whether delivery of your notifications are prevented, delayed or blocked.

17.4. You may not use Amazon SNS to send SMS messages that include Premium Content (as defined in the Mobile Marketing Association Guidelines). You may not charge recipients for receiving Amazon SNS notifications by SMS unless you have obtained the recipient's express consent. You must advise recipients receiving Amazon SNS notification by SMS that wireless carriers may charge the recipient to receive Amazon SNS notifications by SMS. You must obtain our prior written consent before using Amazon SNS to send SMS messages for:

- financial transactions or payment services (e.g., mobile banking, bill presentment, bill payment, money transfer, peer-to-peer payment or lending credit, debit or stored value payment services);
- charitable programs (e.g., soliciting donations for a non-profit organization);
- sweepstakes or contests;
- advertisements or promotions for commercial products, goods or services; or
- location-based services (e.g., where a recipient receives messages based on the geographical location of the recipient's wireless device).

17.5. Any third party push notification platform that you use in connection with Amazon SNS is Third Party Content under the Agreement, and features of Amazon SNS that depend on such platforms may not be secure, uninterrupted or error-free. Your use of such push notification platform is subject to the platform's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change,

discontinue or deprecate support for a push notification platform for any reason at any time.

17.6. You and any of your applications that use Amazon SNS must comply with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

17.7. Through your use of Amazon SNS you will not:

- Transmit any material that contains viruses, Trojan horses, worms or any other malicious, harmful, or deleterious programs.
- Offer or purport to offer any Emergency Services. “Emergency Services” means services that allow a user to connect with emergency services personnel or public safety answering points such as 911 or E911 services.
- Materially violate or facilitate the material violation of any local or foreign law, rule, regulation or order, including laws regarding the transmission of data or software
- Transmit material that is sexually explicit, relates to “adult services”, or contains sensitive financial or identifying information (such as social security numbers)
- Resell, sublicense or timeshare the Services or use them on behalf of anonymous or other third parties.
- Use the Services in hazardous environments (such as operation of nuclear facilities, aircraft navigation, or any other use that may result in foreseeable risk of injury, death, or destruction of property).

18. Consolidated Billing

18.1. You may only use Consolidated Billing as described in this Section and on the AWS Site to (i) link an AWS account (the “Paying Account”) with another AWS account (each, a “Linked Account”), or (ii) allow an AWS account to be linked to a Paying Account. You may only link accounts held by you, your affiliates or your employees, or by your agents or subcontractors currently doing work on your behalf. If an agent or subcontractor ceases doing work on your behalf, you will promptly unlink the applicable account. When accounts are linked, the Paying Account will be billed for and will pay all applicable charges for each Linked Account in accordance with the payment provisions in the Agreement while the accounts are linked. By linking your Linked Account to a Paying Account, you consent to disclosing your billing and account activity for that Linked Account to the Paying Account. We will determine the number of accounts that may be linked. An account may unlink another account from it at any time. As soon as a Linked Account is unlinked from a Paying Account, the Linked Account will be billed for and will pay all applicable charges for the Linked Account in accordance with payment provisions in the Agreement. If a Paying Account is terminated for failure to satisfy the payment provisions in the Agreement, then all linked Accounts associated with the Paying Account will be unlinked. We may unlink a Linked Account from a Paying

Account at any time upon notice to both accounts in accordance with the Agreement, except that accounts linked in violation of this Section 18.1 may be unlinked by us immediately and without notice. Paying Accounts and Linked Accounts are jointly and severally liable for all fees accrued by Linked Accounts while the accounts are linked. Accordingly, if a Paying Account fails to pay for fees accrued by a Linked Account while the accounts are linked, the Linked Account remains liable for such fees.

18.2. When you use the CreateLinkedAccount API to create an AWS account (each, a “Programmatically Created Account”), (i) each Programmatically Created Account is a Linked Account; (ii) the AWS account that you used to access the API is the Paying Account; (iii) except as otherwise provided in the Paying Account’s Agreement, each Programmatically Created Account is governed by the terms of the [AWS Customer Agreement](#); (iv) except as otherwise authorized by AWS, each Programmatically Created Account may be used only by you or your agents or contractors performing work on your behalf and may not be created for any third party; (v) only AWS may unlink a Programmatically Created Account from the Paying Account; and (vi) you are responsible for ensuring that users abide by the terms governing each Programmatically Created Account and for all activities that occur under such account.

19. AWS Identity and Access Management (IAM)

19.1. You may use IAM to create additional sets of security credentials (the “User Credentials”) under your AWS account, the format of which may include a username and password, roles, policies, permissions, access keys, and/or a security token. The User Credentials are subject to change: (a) by you through the IAM APIs, or (b) if we determine in our reasonable discretion that a change is necessary. We will promptly notify you of any change we make to the User Credentials.

19.2. You will ensure that all use of the Services under the User Credentials complies with the terms and conditions of the customer agreement between you and us that governs your use of the Services.

19.3. You are responsible for all applicable fees associated with use of the Services in connection with IAM, including fees incurred as a result of any User Credentials. You are responsible for maintaining the secrecy and security of the User Credentials (other than any key that we expressly permit you to use publicly). You are solely responsible, and we have no liability, for any activities that occur under the User Credentials, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of all User Credentials created under your AWS account, including credentials that you have used IAM to create or disclose to other parties.

19.4. Except as otherwise provided by AWS, you may only use User Credentials for your internal use and may not expose your User Credentials publicly. You may not sell, transfer or sublicense or authorize the creation of User Credentials (other than public use of any key that we expressly permit you to use publicly) to any other party; provided that, you may disclose or cause to be disclosed User Credentials to your agents or subcontractors that are performing services for you, solely to allow the agents or

subcontractors to use the Services on your behalf in accordance with the agreement between you and us that governs your use of the Services.

19.5. Any third party identity provider that you use in connection with the Service Offerings is Third Party Content under the Agreement and may be provided directly to you by a third party under separate terms and conditions. You are solely responsible for complying with those terms and conditions. We may change, discontinue or deprecate support for an identity provider for any reason, including if the continued use of the identity service (a) poses a security or intellectual property issue, (b) is economically or technically burdensome, or (c) must be terminated to comply with the law or requests of governmental entities.

20. Amazon Route 53

20.1. You may use Amazon Route 53 to answer Domain Name System (DNS) queries for your applications.

20.2. You will not create a hosted zone for a domain that you do not own or have authority over.

20.3. All DNS records (other than Private DNS records) used in connection with Amazon Route 53 will be publicly available and AWS will have no liability for disclosure of those DNS records.

20.4 Domain name registration services are provided under our [Domain Name Registration Agreement](#).

21. AWS Elastic Beanstalk

21.1. The URL used in connection with an AWS Elastic Beanstalk environment will have the formulation [myapp].elasticbeanstalk.com. You will select the “myapp” portion of the URL and will not:

- include any trademark of Amazon or its affiliates, or a variant or misspelling of a trademark of Amazon or its affiliates – for example, “endlessboots”, “amaozn”, “smallpartsstore”, “amazonauctions”, “kindlemagazines”, or “kindlewirelessreader” would be unsuitable; or
- otherwise violate the intellectual property rights of any third party or the AWS Acceptable Use Policy (including, without limitation, containing any offensive, harmful or illegal content).

AWS may reject any URL that fails to comply with this Section. Further, AWS may modify any URL in order to make it compliant with this Section. In addition, AWS may treat any URL that fails to comply with this Section as Prohibited Content.

21.2. The [myapp] portion of the URL is reserved for you only during the time your application environment is running. If you stop running your application environment at any time, for any reason, the [myapp] portion of the URL you were using to run the application environment will no longer be available to you, and will be returned to a pool from which it may be used by another AWS customer.

21.3. AWS may make available reference or sample applications for you to use in connection with AWS Elastic Beanstalk (“Elastic Beanstalk Sample Apps”). Elastic Beanstalk Sample Apps are provided “as is” and you will be charged the same fees for running Elastic Beanstalk Sample Apps as you would be charged for running your own application.

21.4. AWS Elastic Beanstalk is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS Elastic Beanstalk.

22. Amazon Simple Email Service (SES)

22.1. We take steps to increase the security and reliability of email you send, attempt to send, or receive using SES (“SES Email”). Like many email service providers, when you send, attempt to send, or receive an email, we (or our third-party providers) may store and scan your SES Email and Your Content included in SES Email. This helps us protect you and SES by preventing and blocking “spam” e-mails, viruses and spyware, and other harmful or unwanted items from being sent and received over SES.

22.2. Your use of SES and all SES Email must comply with the AWS Acceptable Use Policy and the Agreement. We may throttle, suspend or terminate your access to SES, or block or decline to send and/or receive any SES Email, if we determine in our sole discretion that

- our scan of SES Email or Your Content included in SES Email reveals abusive or low quality email (such as “spam”),
- SES Email bounces back to us or we receive abuse complaints (including complaints from third parties) in connection with your SES Email,
- the source or ReturnPath email address you have provided us for “address bounces” or complaints is not successfully receiving email, or
- your use of SES Email does not comply with the AWS Acceptable Use Policy or the Agreement, or
- your SES Emails or Your Content include an attachment in a format that we do not support.

22.3. Your SES Emails may be blocked, delayed or prevented from being delivered by destination email servers and other reasons outside of our control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed or blocked.

22.4. You are solely responsible for ensuring any emails you send and receive using SES comply with the Federal CAN-SPAM Act. AWS is not the “sender” as defined in the Federal CAN-SPAM Act. You will not use SES in connection with an open mail relay, including, without limitation, an open mail relay in the form of an SMTP server, unrestricted web form, or otherwise.

22.5. Your SES Emails may be blocked, delayed or prevented from being received due to your configuration of the Service. You are solely responsible for the proper configuration of the Service to ensure the receipt of emails.

23. AWS CloudFormation

23.1. You may use AWS CloudFormation to create a collection of AWS resources and provision them.

23.2. AWS may make sample templates available for you to use in connection with AWS CloudFormation. All sample templates are offered “as is” and you are solely responsible for your use of the sample templates.

23.3. Any templates you use in connection with AWS CloudFormation must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

23.4. AWS CloudFormation is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS CloudFormation.

24. AWS Direct Connect

24.1. You may use AWS Direct Connect to establish a dedicated network connection between your network and your AWS resources by using connection types and locations supported by AWS. When you establish a dedicated connection, your network traffic that would have otherwise been routed over the Internet may be routed through your dedicated network connection, including your network traffic sent to or from (i) services offered by other affiliates of Amazon.com, Inc. or (ii) the AWS resources of other AWS customers.

24.2. The hardware and equipment you use with AWS Direct Connect must comply with the Documentation provided by AWS. You are responsible for protecting your AWS Direct Connect connections, including using physical security, firewalls and other network security tools as appropriate.

24.3. AWS will permit data center operator or other service provider to connect your hardware to AWS’s hardware at the AWS Direct Connect location(s) that you select. AWS will provide the necessary information to enable the data center operator or other service provider to establish and monitor this connection, including your name, email address, network configuration, activity information, and AWS account number.

24.4. You are responsible for your separate relationship with the data center operator or other service provider, including compliance with your agreement with, and the policies and procedures of, the data center operator or other service provider, and payment of applicable fees to the data center operator or other service provider. You are responsible for providing or procuring (and AWS will not own) any equipment or cabling necessary to establish this dedicated connection. Neither AWS nor any of its affiliates are responsible for the actions, errors or omissions of any employees or contractors of

data center operators or service providers, including if the employees or contractors fail to follow instructions from you or AWS.

24.5. We may disconnect your AWS Direct Connect connection at any time for any reason. If the connection you establish as part of AWS Direct Connect is temporarily unavailable or terminated, AWS will route traffic bound for your AWS resources over the public Internet and AWS's standard data transfer charges will apply. However, if you are using Amazon Virtual Private Cloud (VPC), traffic bound for your Amazon VPC resources will be routed through an IPsec VPN connection. If an IPsec VPN connection is unavailable, traffic bound for your Amazon VPC resources will not be delivered.

25. Amazon ElastiCache

25.1. You may only use Amazon ElastiCache to store, query, retrieve and serve Your Content. You are solely responsible, for the proper configuration of all security settings associated with Amazon ElastiCache.

25.2. You may not access or tamper with any software we install on the cache nodes as part of Amazon ElastiCache.

25.3. Amazon ElastiCache is designed for the ephemeral storage of Your Content. You are responsible for maintaining a persistent data storage for Your Content, and routinely archiving Your Content to prevent the loss of Your Content.

25.4. Replacement cache nodes automatically generated by Amazon ElastiCache may have different IP address, and you are responsible for reviewing your application configuration to ensure that your cache nodes are associated with the appropriate IP addresses.

25.5. We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the cache nodes as part of Amazon ElastiCache.

25.6. Reserved Cache Node Pricing. You may designate Amazon ElastiCache cache node as subject to the reserved pricing and payment terms ("Reserved Cache Node Pricing") set forth on the Amazon ElastiCache detail page on the AWS Site (each designated instance, a "Reserved Cache Node"). You may designate cache nodes as Reserved Cache Nodes by calling to the Purchasing API or selecting the Reserved Cache Node option in the AWS console. When you designate a cache node as Reserved Cache Node, you must designate a region, cache node type, Reserved Cache Node type, and quantity for the applicable Reserved Cache Node. The Reserved Cache Node may only be used in the designated region. We may change Reserved Cache Node Pricing at any time but price changes will not apply to previously designated Reserved Cache Nodes. We may terminate the Reserved Cache Node Pricing program at any time. Reserved Cache Nodes are nontransferable and all amounts paid in connection with the Reserved Cache Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Cache Node type, or terminate the Reserved Cache Node Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any

previously designated Reserved Cache Nodes. Upon expiration or termination of the term of a Reserved Cache Node, the Reserved Cache Node Pricing will expire and standard on-demand usage prices will apply to the cache node. In addition to being subject to Reserved Cache Node Pricing, Reserved Cache Nodes are subject to all data transfer and other fees applicable under the Agreement.

26. AWS Support

26.1. We will provide “Support” in accordance with the terms of AWS Support Features page available at <http://aws.amazon.com/premiumsupport> (the “Guidelines”). AWS Support is available only as described in the Guidelines. If you are experiencing problems with one or more Services in connection with your use of any Content that was provided to you by a third party (someone other than yourself or AWS) then AWS Support is not available.

26.2. In providing AWS Support, AWS will use commercially reasonable efforts to (a) respond within the “Response Times” set forth in the Guidelines for all properly submitted cases from authorized individuals, and (b) work towards the identification and resolution of the problems submitted. When submitting a case, you may designate the severity level of a problem; provided that, we reserve the right to reclassify the severity level in our reasonable opinion. All Response Times are measured from the point when a case has been properly submitted by an authorized individual to us. Cases may be submitted as specified in the Guidelines. We do not represent, warrant or guarantee that (i) we will always be able to resolve a case fully, (ii) you will no longer experience a problem, (iii) we will provide a bug fix, patch or other workaround in connection with the identified problem, or (iv) any support or advice will result in any performance efficiency or improvement. You are solely responsible for the implementation and results of any suggestions or advice received.

26.3. Unless otherwise set forth in the Guidelines, AWS Support fees will be the greater of (a) the specified minimum monthly fee, or (b) a percentage of your monthly usage charges for all Services during the billing period. Regardless of when you sign up or terminate AWS Support, you are obligated to pay for a minimum of thirty (30) days of support each time you register to receive the service. Implementation of any suggested configurations or improvements may result in additional fees and charges. We reserve the right to refuse to provide AWS Support to any customer that frequently registers for and terminates the service.

27. AWS GovCloud (US) Service Terms

27.1 You are responsible for satisfying any applicable eligibility requirements for using the AWS GovCloud (US) Region including providing accurate and current registration information. We may require you to provide additional registration information before we permit you to access the AWS GovCloud (US) Region. Such information may include your U.S. person status, as defined by 22 CFR part 120.15 (“US Person”), and whether you are subject to export restrictions under U.S. export control laws and regulations. We may make, directly or through third parties, any inquiries we consider necessary to validate information that you provide to us, including without limitation checking

commercial and/or governmental databases. While we may take steps to verify the identity of our Customers, we cannot and do not guarantee any Customer's identity.

27.2 AWS is responsible for maintaining access controls to the AWS GovCloud (US) Region that limit AWS personnel's physical and logical access to the "AWS Network" to US Persons only. The AWS Network consists of AWS's internal data center facilities, servers, networking equipment, and host software systems that are within AWS's reasonable control and are used to provide the AWS Services. You are responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer or End User account access, data transmission, encryption, and appropriate storage and processing of your Content within the AWS GovCloud (US) region. AWS makes no representation or warranty related to the US Persons status of any Customer or End Users that may be granted access to the AWS GovCloud (US) Region by other Customers and their End Users.

27.3 You are responsible for verifying the adequacy of the AWS GovCloud (US) Region for the processing and storage of your Content and that your use of AWS Services will comply with the laws and regulations that may govern your Content. You are also solely responsible for verifying that End Users are eligible to access your Content in the AWS GovCloud (US) region.

27.4 You may only use Amazon VPC to connect your computing resources to the AWS GovCloud (US) region.

27.5 AWS Services may not be used to process or store classified data. If you or your end users introduce classified data into the AWS Network, you will be responsible for all sanitization costs incurred by AWS.

28. Amazon DynamoDB

28.1 You will be charged for the throughput capacity (reads and writes) you provision in your Amazon DynamoDB tables even if you do not fully utilize the provisioned capacity.

28.2 The actual reads and writes performance of your Amazon DynamoDB tables may vary and may be less than the throughput capacity that you provision.

28.3 Reserved Capacity Pricing. You may purchase reserved throughput capacity (reads and writes) subject to the pricing and payment terms set forth on the Amazon DynamoDB detail page on the AWS Site ("Amazon DynamoDB Reserved Capacity"). You may purchase Amazon DynamoDB Reserved Capacity by submitting a request through the AWS console. When you purchase Amazon DynamoDB Reserved Capacity, you must designate a region, quantity, and term. You will be charged (1) a one-time, up-front fee and (2) an hourly fee for each hour during the term based on the amount of Amazon DynamoDB Reserved Capacity you purchase. The Amazon DynamoDB Reserved Capacity may only be used in the designated region and only by the account that purchased the Amazon DynamoDB Reserved Capacity. We may change the pricing for Amazon DynamoDB Reserved Capacity at any time, but price changes will not apply to previously purchased Amazon DynamoDB Reserved Capacity. We may terminate the Amazon DynamoDB Reserved Capacity program at any time.

Amazon DynamoDB Reserved Capacity is nontransferable and all amounts paid in connection with the Amazon DynamoDB Reserved Capacity are nonrefundable, except that if we terminate the Agreement (other than for cause) or the Amazon DynamoDB Reserved Capacity program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously purchased Amazon DynamoDB Reserved Capacity. Upon expiration or termination of the term of any Amazon DynamoDB Reserved Capacity, standard on-demand usage prices will apply to the your use of Amazon DynamoDB. Amazon DynamoDB Reserved Capacity is also subject to all storage, data transfer and other fees applicable under the Agreement.

28.4 You may install the local version of DynamoDB only on computer equipment owned or controlled by you and may use it solely (a) for your internal business purposes and (b) in connection with the Services. Your use of DynamoDB Local is governed by the DynamoDB Local License Agreement, located here: [DynamoDB Local License Agreement](#).

29. AWS Storage Gateway

29.1 You may only use the AWS Storage Gateway on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Storage Gateway is governed by the AWS Storage Gateway License, located here: [AWS Storage Gateway License Agreement](#).

30. AWS Marketplace

30.1 The AWS Marketplace is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content of third parties offered through the AWS Marketplace constitutes “Third Party Content” under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

30.2 Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

30.3 AWS may stop providing the AWS Marketplace (or any features of or listings within the AWS Marketplace) to you at AWS’s sole discretion, without prior notice to you. In

addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

30.4 You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace. This may include one-time payments as well as recurring payments. A “recurring payment” is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g. annually or monthly). The applicable fees and billing periods for the Content are listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. You may cancel your subscriptions at any time by logging into “Your Software Subscriptions” on the AWS Site. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

31. AWS Data Pipeline

31.1 You may only use the AWS Data Pipeline on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services.

31.2 Your use of the AWS Data Pipeline Remote Runner is governed by the AWS Data Pipeline Remote Runner License, located here: [AWS Data Pipeline Remote Runner License Agreement](#).

32. Amazon Elastic Transcoder

32.1 The further distribution of files created by Amazon Elastic Transcoder may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining these licenses and paying any necessary royalties or fees.

32.2 We do not represent, warrant or guarantee the quality of any files you create through your use of Amazon Elastic Transcoder or that the files will be of a certain fidelity or error free.

33. AWS OpsWorks

33.1 You may use AWS OpsWorks to create a collection of AWS resources and provision them.

33.2 AWS may make sample templates available for you to use in connection with AWS OpsWorks. Sample templates may include chef recipes and/or sample code. All sample templates are offered “as is” and you are solely responsible for your use of the sample templates.

33.3. Any templates you use in connection with AWS OpsWorks must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

33.4. In addition to any charges you incur for your use of AWS Opsworks, you are responsible for all fees incurred for AWS services used in connection with AWS OpsWorks.

33.5. You may install and use the AWS Opsworks agent solely with AWS Opsworks. Your use of the AWS Opsworks agent is governed by the AWS Opsworks Client License Agreement, located here: [AWS Opsworks Client License Agreement](#).

34. AWS CloudHSM

34.1 You may not access, modify, update or tamper with, or attempt to access, modify, update or tamper with, any of the software installed on the HSM device, except as expressly permitted by us.

34.2 As part of the AWS CloudHSM service, AWS will provide access to HSM devices of its choosing. You have no ownership or rental rights in the specific HSM device to which we provide you access in the course of providing the AWS CloudHSM service.

34.3. In conjunction with the AWS CloudHSM service, you may be allowed to use certain software (including related documentation) developed and owned by SafeNet, Inc. or its licensors (collectively, the “SafeNet Software”). In connection with your use of the SafeNet Software, SafeNet and its licensors require that you agree to the additional terms and conditions located [here](#) .

34.4. If you elect to discontinue use of a HSM device, you must issue a command to delete the contents of the device (i.e., “zero-ize” the device). You will continue to be charged for use of an HSM device until the device has been zero-ized out and you notify us that you wish to discontinue the service.

34.5. Failure of an HSM device can result in unrecoverable data loss. We do not perform backups or implement fault tolerant configurations on your behalf. You are solely responsible for backup and fault tolerant configurations.

35. Amazon AppStream

35.1. When you use AppStream, you also use Amazon EC2, CloudWatch and AutoScaling, S3, and DynamoDB, and your use of AppStream is subject to all the terms that govern those services.

35.2. The software and other content that you upload to run on AppStream (including your AppStream hosted application, dependencies and installer), your AppStream entitlement service, and your AppStream client software are Your Content. The use of Your Content with AppStream, including the transmission of internet video and your distribution of any video decoder in your AppStream client software, may require that you obtain license rights from third parties. You are solely responsible for obtaining necessary licenses and paying any necessary royalties or fees applicable to Your Content.

35.3. Using NVIDIA Software. Use of the graphics processing unit (GPU) of an EC2 instance requires that you use driver software developed and owned by NVIDIA

Corporation or its licensors (collectively, the “NVIDIA Software”). If your AppStream application uses the GPU on an EC2 instance, NVIDIA and its licensors require that you agree to these additional terms and conditions:

- Your use of the NVIDIA Software is subject to the terms and conditions of the License for Customer Use of NVIDIA Software, currently located at <http://www.nvidia.com/content/DriverDownload-March2009/licence.php?lang=us> (the “NVIDIA License”). By using the NVIDIA Software, you hereby agree to be bound by the terms of the NVIDIA License.

35.4. We may collect information about Your Content’s use of AppStream, including CPU and GPU utilization, memory usage, IO performance, client type, client session length, transmission latency, client geographic and network locations, video and audio quality, and error and information messages.

35.5. AppStream Stand-Alone; AppStream Materials. We may make AppStream software and other materials (“AppStream Materials”) available to you on instances running in your own AWS account (“AppStream Stand-Alone”). AppStream Stand-Alone may only be used for your evaluation, development and testing purposes, and not for streaming your application to third party end users. AppStream Stand-Alone may enable you to direct us to pre-install certain third-party software on the instance via the applicable CloudFormation template. That third-party software may be subject to separate license terms and you are solely responsible for complying with those terms. AppStream Materials used on AppStream Stand-Alone are AWS Content and are subject to the license restrictions set out in the Agreement. You will only use the AppStream Materials on the AppStream Stand-Alone instance, and you will not download, transmit, or otherwise remove the AppStream Materials from AppStream Stand-Alone instances.

36. Amazon WorkSpaces

36.1. Any Content that you or any End User run on, cause to interface with, or upload to your WorkSpaces is Your Content. You are responsible for maintaining licenses and adhering to the license terms of any of Your Content on your WorkSpaces.

36.2. Using Microsoft Software. In conjunction with the Services, you and your End Users may be allowed to use Microsoft Software. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to the additional terms and conditions specified in section 4.2 above.

36.3. You and End Users may only use the WorkSpaces Services for an End User’s personal or office productivity. WorkSpaces are not meant to accept inbound network connections, be used as server instances, or serve web traffic or your network traffic. You may not reconfigure the inbound network connections of your WorkSpaces. We may shut down WorkSpaces that are used in violation of this section or other provisions of the Agreement.

36.4. You and End Users may only use the WorkSpaces client software on computer equipment owned or controlled by you or your End Users for your internal business

purposes, solely to access Your Content used in connection with the Services. Your use of the WorkSpaces client software is governed by the WorkSpaces Client Software License Agreement located here: <http://help.amazonworkspaces.com/app-terms.html>.

36.5. As part of regular operation the Service will be able to perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks the Service will use programmatic access that is provisioned as part of the Workspace creation. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

36.6. The charges for the Service apply on a monthly basis. If a Workspace is launched after the first of a month, then the monthly price for that Workspace will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a Workspace is terminated before the end of a month, then the monthly charge will still apply.

36.7. The charges for the Service include the cost of streaming data between your WorkSpaces and End Users' devices unless you stream via VPN, in which case you will be charged VPN data transfer rates in addition to any applicable Internet data transfer charges. Other Workspace data transfer will be charged using Amazon EC2 data transfer pricing.

36.8. You may not attempt to tamper with any software we pre-load on the Workspace instance (including the operating system software running on the Workspace), or in a way that is not part of normal operations or that attempts to circumvent charges for the Service. During the regular operation of the Service, software installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with or use this license activation server in a way that is not part of normal operations or that attempts to circumvent charges for the Service. We may block access to the Service, and suspend your account, if we determine that you are in violation of this section.

36.9. As part of regular operation of the service, WorkSpaces may be updated with latest operating system and software patches. During such updates, only software, documents, and settings that are part of the OS image used for the Workspace or part of a user's profile (D: drive in the Workspace) will persist.

36.10. Microsoft BYOL Licensing. Under this option, Amazon WorkSpaces enables you to provision WorkSpaces using your Microsoft Software and Microsoft Licenses (the "WorkSpaces BYOL Program"). You must be eligible to use the WorkSpaces BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using Microsoft Software under the WorkSpaces BYOL Program, you agree to the Microsoft EULA. You agree that you have determined that your use of the WorkSpaces BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted. AWS recommends that you consult with your

own advisors to understand and comply with the applicable Microsoft licensing requirements.

36.11. You are responsible for End Users use of your WorkSpaces. You are responsible for determining End User policies and configuring End User policy controls for WorkSpaces.

37. Amazon Cognito

37.1 Any third party identity provider that you use in connection with Amazon Cognito is Third Party Content under the Agreement, and features of Amazon Cognito that depend on such identity providers may not be secure, uninterrupted or error-free. Your use of such an identity provider is subject to the provider's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change, discontinue, or deprecate support for an identity provider for any reason and at any time.

37.2 You are responsible for (a) providing legally adequate privacy notices to your end users; (b) obtaining any necessary consent from the end user for the collection, use, transfer, and storage of any name, password, other login information, or personally identifiable information or personal data of any end user that you (or any third-party plug-in or service provider you use) may access; (c) using and authorizing others to access and use the information only for the purposes permitted by the end user; and (d) ensuring the information is collected, used, transferred, and stored in accordance with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

38. Amazon WorkDocs

38.1 You will need an AWS account to start using the Service Offering. Once you have enabled Amazon WorkDocs under your account, End Users can be invited to join, sign up, and start using the Service Offering under your account without each one having a separate AWS account.

38.2 You are responsible for paying the fees for use by you and your End Users of the Service Offering associated with your AWS account.

38.3 Within the Service Offering, your End User accounts are managed by End Users with administrative privileges ("WorkDocs Administrators"). These WorkDocs Administrators can access information about the accounts of other End Users, such as when they last logged in, what documents they viewed, etc. These WorkDocs Administrators can also deactivate other End Users' accounts and control access to certain functionality, such as restricting the ability to share files with external domains or changing their storage limits.

38.4 We may limit the number of versions that you can store for each file. We will announce any change in limits to the number of versions that you may store in advance of implementing those limits.

38.5 We may delete, without liability of any kind, any of your End Users' data or Content uploaded to Amazon WorkDocs if the End User is marked "Inactive" in Amazon WorkDocs' Administrator Dashboard and has not been billed for more than 60 days. We may also delete your Amazon WorkDocs site and Content when you have no End Users marked "Active" within Amazon WorkDocs Administrator Dashboard for more than 60 days.

38.6 If no End User accounts associated with your AWS account have registered any usage of the Service Offering for several months, then we may delete the inactive End Users' accounts after providing 30 days' notice.

38.7 You and your End Users may not use the Service Offering to host any files that violate the AWS Acceptable Use Policy. If we determine, in our sole discretion, that your use of the Service Offering may be in violation of the AWS Acceptable Use Policy or the Agreement, then we may delete those files.

38.8 Your use of the Amazon WorkDocs Sync Software is governed by the Amazon WorkDocs Sync License Agreement found here:[Amazon WorkDocs Sync License Agreement](#) .

38.9 Your use of an Amazon WorkDocs Application is governed by the Amazon WorkDocs Application License Agreement found here:[Amazon WorkDocs Application License Agreement](#) .

38.9 Your use of the Amazon WorkDocs Web Clipper is governed by the Amazon WorkDocs Web Clipper License Agreement found here:[Amazon WorkDocs Web Clipper License Agreement](#) .

39. Mobile Analytics

39.1 Your Data; Privacy. You are solely responsible for all information and data you collect or store using Mobile Analytics ("Your Data"). Your Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your Data (including by us), and (b) collect, use, transfer, and store Your Data in accordance with any privacy notice you provide, and all applicable laws.

40. AWS Config

40.1 You are responsible for all fees incurred for Services, such as Amazon SNS and Amazon S3, used in connection with AWS Config.

41. AWS CodeDeploy

41.1 AWS CodeDeploy to Amazon EC2 instances is offered at no additional charge but requires the use of other AWS Services. AWS CodeDeploy to on-premises instances is offered at the then current fees and charges that are posted on the AWS CodeDeploy detail page on the AWS Site; and may also be used with other AWS Services. You are responsible for all fees incurred for Services used in connection with AWS CodeDeploy.

41.2 AWS may make available reference or sample AppSpec configuration files and applications for you to use in connection with AWS CodeDeploy. These files and applications are provided “as is”, and you are solely responsible for your use of such files and applications. You will be charged the same fees for running them as you would be charged for running your own application.

42. AWS Lambda

42.1 You are responsible for Your Content, including (a) the performance of software you use with AWS Lambda and any reference libraries we provide and (b) maintaining licenses and adhering to the license terms of any software you run.

42.2 You are responsible for all fees incurred for Services used in connection with AWS Lambda.

42.3 We may delete, upon 30 days’ notice to you and without liability of any kind, any of Your Content uploaded to AWS Lambda if it has not been run for more than three (3) months.

43. Amazon WorkMail

43.1 The charges for the Service apply on a monthly basis. If an End User account is created after the first of a month, then the monthly fee for that mailbox will be adjusted on a pro rata basis from the first day it was active to the end of that month. If an End User account is terminated or deleted before the end of a month, then the monthly fee for that End User account will still apply. You are responsible for paying the fees for all End User accounts associated with your AWS account.

43.2 Amazon WorkMail allows you to register a test mail domain (e.g. <yourname>.awsapps.com). You can use the test mail domain as long as you are using Amazon WorkMail. If you stop using Amazon WorkMail, the test mail domain may become available to be registered and used by other Customers. You cannot use the test mail domain for other purposes outside of Amazon WorkMail.

43.3 If your use of Amazon WorkMail is terminated, we may delete your data and your End Users’ mailboxes.

43.4 When you use Amazon WorkMail, you also use AWS Key Management Service, AWS IAM, and Amazon SES, and your use of Amazon WorkMail is subject to the terms that govern those services. You are responsible for the separate fees you may accrue for using AWS Key Management Service.

43.5 Amazon WorkMail provides a filtering service designed to filter unwanted emails, such as spam, phishing emails, and email infected with viruses. You acknowledge that the technological limitations of the filtering service will likely result in the capture of some legitimate email, and the failure to capture some unwanted email, including email infected with viruses.

43.6 Your mail domain and End Users’ accounts may be blocked, delayed or prevented from being delivered by destination email servers and other reasons outside of our

control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed, or blocked.

43.7 You agree not to use Amazon WorkMail for sending:

- Bulk emails, such as mass marketing emails
- Unsolicited and unwanted emails
- Phishing emails

43.8 Your use and your End Users' use of Amazon WorkMail must comply with the AWS Acceptable Use Policy, applicable law, and the Agreement. You are solely responsible for understanding and complying with the legal and regulatory requirements applicable to your business. You are solely responsible for ensuring any emails you or your End Users send using Amazon WorkMail comply with the Federal CAN-SPAM Act and all other applicable law. You agree that AWS is not the "sender" of any emails you or your End Users send using Amazon WorkMail as defined in the Federal CAN-SPAM Act and all other applicable laws.

43.9 Amazon WorkMail may log and use information such as server hostnames, IP addresses, timestamps, mail queue file identifiers, and spam filtering information for the purpose of troubleshooting or improving Amazon WorkMail.

44. Amazon Machine Learning

44.1 You may only use Amazon Machine Learning ("Amazon ML") to process Your Content. You are solely responsible for the proper configuration of all security settings associated with Amazon ML.

44.2 We retain all rights to all improvements we make to any Amazon websites or technologies, including any and all improvements resulting from or related to Amazon ML processing Your Content.

44.3 We may delete, without liability of any kind, any Amazon ML object that remains inactive for more than the number of days specified in the user documentation.

44.4 You are responsible for all fees incurred from your use of Amazon ML regardless of the quality of the results obtained. Your use of Amazon ML requires the use of other Services. You are responsible for all fees incurred for Services used in connection with Amazon ML.

45. Amazon WorkSpaces Application Manager (Amazon WAM)

45.1 Any Content that you or any End User run on, cause to interface with, or upload to Amazon WorkSpaces Application Manager (Amazon WAM) via the Amazon WAM Admin Studio is Your Content.

45.2 You are responsible for maintaining licenses and adhering to the license terms of any of Your Content delivered via Amazon WAM to your WorkSpaces.

45.3 As part of regular operation of Amazon WAM, the Service will be able to perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks the Service will use programmatic access that is provisioned as part of Amazon WAM. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

45.4 As part of regular operation of Amazon WAM, the Service will use the End User and machine identity that is part of your AWS Directory Services environment to check for content that an End User is entitled to use. In addition, content installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with this license activation server, or use it in a way that is not part of normal operations or that attempts to circumvent this Service. We may block access to this Service, and suspend your account, if we determine that you are in violation of this Section.

45.5 The charges for the Service apply on a monthly basis. If Amazon WAM is enabled for an End User after the first of a month, then the monthly price for that End User's subscription will be adjusted on a pro rata basis from the first day it was active to the end of that month. If Amazon WAM is disabled for an End User before the end of a month, then the entire monthly charge will still apply.

45.6 When you use Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you may also use other AWS Services, and use of other AWS Services is subject to the terms that govern those Services. In addition to any charges you incur for your use of Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you are responsible for all fees incurred for AWS Services used in connection with Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications.

45.7 Amazon WAM Admin Studio, Amazon WAM Admin Player, and Amazon WAM desktop applications are AWS Content and may not be manipulated or reverse engineered in any way.

45.8 You may use the Amazon WAM Admin Studio only to package applications, and the Amazon WAM Admin Player only to validate applications, that will be delivered via Amazon WAM to your WorkSpaces. You may not tamper with either of those applications that we preload as part of the Amazon WAM Admin Studio or Player, the underlying Amazon EC2 AMI, or use the Amazon WAM Admin Studio or Player in a way that is not part of normal operations or that attempts to circumvent this Service.

45.9 You may not attempt to tamper with any software that is part of the Amazon WAM service that we preload on the Workspace instance, or use it in a way that is not part of normal operations or that attempts to circumvent this Service.

45.10 As part of regular operation of the Service, we may update Amazon WAM desktop applications with software patches.

45.11 You are responsible for End Users use of Amazon WAM. You are responsible for determining End User policies and configuring End User policy controls for using applications via Amazon WAM.

46. AWS Marketplace for Desktop Apps

46.1 The AWS Marketplace for Desktop Apps is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may be sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content.

46.2 Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

46.3 AWS may stop providing the AWS Marketplace for Desktop Apps (or any features of or listings within the AWS Marketplace for Desktop Apps) to you at AWS's sole discretion, without prior notice to you. In addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

46.4 You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace for Desktop Apps. This may include one-time payments as well as recurring payments. A "recurring payment" is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g., annually or monthly). The applicable charge for the Content is listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. If a subscription is purchased after the first of a month, then the monthly price for that Content will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a subscription is cancelled before the end of a month, then the entire monthly charge will still apply. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

46.5 Third-party support information for each subscription, if any, is set forth on the detail page for the Content. While AWS may help facilitate the resolution of disputes between you and third-party Content creators, for the Content, AWS does not guarantee the quality, safety or legality of items advertised, and support for the Content is the obligation of the third-party Content creator.

46.6 If the Content is offered, sold, or resold by AWS, then it is subject to the terms on the Content's detail page. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content offered or sold by third parties through the AWS Marketplace for Desktop Apps constitutes "Third Party Content" under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth

or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

47. AWS Directory Service

47.1 In conjunction with your use of AWS Directory Service, you and your End Users may be allowed to use Microsoft Software. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to the additional terms and conditions specified in Section 4.2 above.

47.2 If your AWS account is suspended for sixty (60) days or more, we may delete, without liability of any kind, Your Content and directories that are stored in AWS Directory Service upon thirty (30) days prior notice to you.

47.3 We may terminate your AWS Directory Service directory instance if you attempt to access, tamper with, or modify any software or configuration we pre-load on the directory instance, including the operating system software running on the directory instance.

48. Amazon API Gateway

48.1 You may use the Amazon API Gateway to publish, maintain, monitor, and secure Your Content at any scale to accept and process concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.

48.2 By using the Amazon API Gateway you acknowledge and agree that established throttling thresholds may vary, cache services may be limited by us in our sole discretion, and version capacity will not exceed 300 deployments per API at any given time. In addition and without limiting your obligations under the Agreement, you agree not to and not to attempt to: (i) access any resources not assigned to you by us; and/or (ii) perform any form of network discovery and/or load testing of Your Content inside the Amazon API Gateway.

48.3 You are solely responsible for the access, operation, performance, and security of all Your Content you use with Amazon API Gateway.

49. AWS Device Farm

49.1 As part of the AWS Device Farm, you may provide us with application package(s), test package(s) (pre-compiled), test script source code, application extension files, and/or auxiliary data files that have been developed by or for you in a format specified by AWS (each, an “App” or “Apps”) for testing on one or more mobile devices, tablets or other devices that we make available through the AWS Device Farm (each, a “Device(s)”). You may select one or more tests in the AWS Device Farm to be performed with your App(s) on the Device(s) you select (a “Test” or “Testing”).

49.2 For any Test run on an Apple Device (each, an “Apple Test”), you represent and warrant that you have an active and valid registered Apple Developer Account under the iOS Developer Program License Agreement with Apple at the time any such Apple Test

is run. You appoint us as your Authorized Developer (as defined in the iOS Developer Program License Agreement) for the duration of all Apple Tests and understand that you are responsible to Apple for all actions we undertake in connection with each Apple Test.

Without limiting your obligations under the Agreement, you agree not to and not to attempt to:

- (i) perform any network discovery inside the AWS Device Farm or otherwise in connection with the Test;
- (ii) access any resources not assigned to you by us (including any Devices);
- (iii) generate any internet traffic from within the EC2 instances of AWS Device Farm, unless approved by us; internet traffic should be limited to Devices only;
- (iv) attempt to establish a direct connection to any Device, nor access or connect to other infrastructure components except as permitted by us;
- (v) root, unlock, or jailbreak any Device;
- (vi) modify any files generated by the AWS Device Farm in a manner that would interfere with any Services;
- (vii) install persistent software on Devices or EC2 instances; and/or
- (viii) factory reset or change settings on Devices nor call and/or access third-party servers in a manner that would interfere with any Services.

49.3 You agree not to rely on any Testing or Report for any purpose, including that any App(s) meet any requirements for inclusion in any application repository of any kind (such as the Apple App Store or Google Play Store). You acknowledge and agree that we may disclose the App(s) to third parties solely for purposes of conducting automated security verification.

49.4 We make no representation as to the availability of the AWS Device Farm. We may change the Tests, Reports or Device(s) offering(s) or any other components or services that are a part of or available through the AWS Device Farm at any time.

50. Amazon Elasticsearch Service

50.1 Amazon Elasticsearch Service creates daily automated snapshots of your Amazon Elasticsearch Service domains. We will maintain these automated snapshots for a period of 14 days after they are created. We may delete automated snapshots, without liability of any kind, at any time after 14 days.

50.2 You may not access or tamper with any software we install on the Amazon Elasticsearch Service domains.

50.3 We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the Amazon Elasticsearch Service domains.

51. AWS Database Migration Service and AWS Schema Conversion Tool

51.1 You may use AWS Database Migration Service solely for the purpose of migrating data to or from Amazon RDS or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the “DMS Supported Services”). Neither you nor any End User may use the Amazon RDS Migration Service to migrate data, directly or indirectly, from a source that is not a DMS Supported Service to a destination that is also not a DMS Supported Service.

51.2 AWS Database Migration Service and the AWS Schema Conversion Tool collect non-personally identifiable metrics regarding your use of the Service Offerings, including the types of database engines used, number of rows processed, duration of the migration or conversion tasks, and migration or conversion task failure status. These metrics may be used by AWS to provide, maintain, and improve the quality and feature set of the Service Offerings.

51.3 The AWS Schema Conversion Tool is AWS Content, and you may install and use it solely for the purpose of migrating your database schemas to Amazon RDS or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the “SCT Supported Services”). Neither you nor any End User may distribute the AWS Schema Conversion Tool or use it to migrate database schemas to a destination that is not an SCT Supported Service. If you would like to use the AWS Schema Conversion Tool to migrate database schemas to a destination that is not an SCT Supported Service, contact us for special pricing.

51.4 AWS Database Migration Service is offered as a preview and is considered a Beta Service, as defined in these Service Terms. Your use of AWS Database Migration Service is subject to the Beta Service Participation terms, as described above.

52. Amazon Inspector

52.1 Amazon Inspector is AWS Content. Neither you nor any End User may, or may attempt to, distribute Amazon Inspector.

52.2 Some components of Amazon Inspector are governed by open source software licenses identified in the notice file accompanying the Amazon Inspector Agent. Your license rights with respect to these individual components are defined by the applicable open source software license.

52.3 Amazon Inspector is offered in a limited preview and is considered a Beta Service as defined in these Service Terms. Your use of Amazon Inspector is subject to the Beta Service Participation terms, as described above.

53. AWS Mobile Hub

53.1 AWS Mobile Hub can be used by you to connect to AWS Service Offerings as made available from time to time by AWS in its sole discretion. Use of the AWS Mobile Hub is subject to AWS Service Offering terms and applicable pricing. You are responsible for maintaining licenses and adhering to the license terms of any software you download and use in connection with AWS Mobile Hub.

54. AWS IoT

54.1 AWS IoT Services that you enable must comport with AWS IoT Developer Guidelines and this Agreement. AWS Developer IoT Guidelines are subject to change at any time without notice.

54.2 The following data guidelines currently apply to Registry and Shadow Data (as referenced in the AWS IoT Developer Guidelines) stored in connection with individual devices and may be changed at any time without notice. Device Shadow Data for an individual device expires and will be deleted if you do not update the Shadow Data for an individual device within 1 year (12 months). Device Registry Data for an individual device expires and will be deleted if you do not update the Registry data for an individual device within 7 years (84 months). Once the Registry and/or Shadow Data has been updated for an individual device the data restriction time frame for an individual device resets and the Registry and/or Shadow Data storage time frame for an individual device starts over.

54.3 You are responsible for all applicable fees associated with use of the Services in connection with AWS IoT. You are solely responsible, and we have no liability, for any activities that occur in the application and/or use of AWS IoT, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of any AWS IoT devices enabled by your AWS account.

55. Amazon QuickSight

55.1 You may enable End Users to use Amazon QuickSight under your account. Termination of your use of Amazon QuickSight, will also terminate such End Users' use of Amazon QuickSight.

55.2 Amazon QuickSight End User accounts are managed by End Users with administrative privileges ("Amazon QuickSight Administrators"). Amazon QuickSight Administrators can (a) activate and deactivate End Users' Amazon QuickSight accounts; (b) control End User access to data sets and certain functionality of Amazon QuickSight; and (c) access information about End Users' use of Amazon QuickSight.

55.3 Amazon QuickSight may use Your Content to make personalized recommendations to you, such as suggested visualizations based on your query history.

55.4 Subject to the Agreement and these Service Terms, you and your End Users may use Amazon QuickSight by logging into quicksight.aws.amazon.com.

55.5 Amazon QuickSight is offered as a preview and is considered a Beta Service, as defined in these Service Terms. Your use of Amazon QuickSight is subject to the Beta Service Participation terms, as described above.

56. AWS Certificate Manager

56.1 By using AWS Certificate Manager (“ACM”) you authorize us, Amazon Trust Services, LLC (“ATS”), or our affiliates (collectively, “Amazon CA”) to apply for and obtain SSL/TLS certificates (each, a “Certificate”) from certification authorities, some of whom may be third parties, for the domain name you provide to us. By submitting a request for a Certificate, you certify that (1) you are the Domain Name Registrant (as defined in the then current CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (the “CA/B Forum Requirements” currently located at <https://cabforum.org/baseline-requirements-documents/>)); (2) you have control over the Fully-Qualified Domain Name (as defined in the CA/B Forum Requirements); or that (3) you have been granted authority by the Domain Name Registrant to authorize Amazon CA to apply for and obtain each Certificate. You acknowledge that, solely for purposes of obtaining the Certificate and for no other purposes, you are giving Amazon CA control over the Fully-Qualified Domain Name, and you approve of it requesting the Certificate for the domain name. We may decline to provide you with a Certificate for any reason.

56.2 You agree that:

- i. All information you provide in connection with your use of ACM is and will be accurate and complete information at all times (and you will promptly notify us if your information changes);
- ii. You will review and verify the Certificate contents for accuracy;
- iii. You may use a Certificate provided to you by us solely on servers that are accessible at the subjectAltName(s) listed in the Certificate and will use the Certificate solely in compliance with all applicable laws;
- iv. You will promptly cease using a Certificate, and promptly notify us, in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
- v. You will promptly cease using a Certificate, and promptly notify us, if the private key associated with the Certificate is, or becomes, subject to a Key Compromise (as defined in the CA/B Forum Requirements) or the Certificate is otherwise subject to misuse;
- vi. You will promptly respond to Amazon CA’s instructions concerning Key Compromise or Certificate misuse;
- vii. You will not modify, sublicense, or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or private key;

- viii. You will not, in connection with use of the Certificate, upload or distribute any files or software that may damage the operation of another's computer;
- ix. You will not make representations about or use a Certificate except as may be allowed in ATS's [CPS](#) ;
- x. You will not, in connection with use of the Certificate, impersonate or misrepresent your affiliation with any entity;
- xi. You will not permit an entity other than Amazon CA to control the Private Key matching the Public Key in the Certificate (where "Private Key" and "Public Key" are defined by the CA/B Forum Requirements);
- xii. You will not use a Certificate to breach the confidence of a third party or to send or receive unsolicited bulk correspondence; and
- xiii. Notwithstanding anything to the contrary in the Agreement, you acknowledge that Amazon CA (or our applicable third-party contractor) may revoke a Certificate at any time, and you agree that you will cease using the Certificate immediately upon our notice of such revocation.

57. Amazon Lumberyard Engine

57.1 Lumberyard Materials. Amazon Lumberyard consists of an engine, integrated development environment, and related assets and tools we make available at aws.amazon.com/lumberyard/downloads or otherwise designate as Lumberyard materials (collectively, "Lumberyard Materials"). The Lumberyard Materials include the "Lumberyard Redistributables" listed at docs.aws.amazon.com/console/lumberyard/userguide/lumberyard-redistributables . Lumberyard Materials are AWS Content. The term "Lumberyard Materials" does not include Content distributed with the Lumberyard Materials under separate license terms (such as code licensed under an open source license).

57.2 License. In addition to the rights granted to AWS Content under the Agreement, we also grant you a limited, non-exclusive, non-sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

a. Development: You may use, reproduce, modify, and create derivative works of the Lumberyard Materials to develop and support video games, software, audio-visual works, and other content (each work created through use of the Lumberyard Materials is a "Lumberyard Project"). Lumberyard Projects, excluding any AWS Content and Third Party Content included therein, are Your Content.

b. Distribution to End Users: You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute (including via third party distributors) to End Users the Lumberyard Redistributables (including any permitted modifications and derivatives) as part of a Lumberyard Project. However, you may do so only if (i) the Lumberyard Project provides material content or functionality beyond that provided by

the Lumberyard Redistributables themselves, (ii) the Lumberyard Redistributables are integrated into the Lumberyard Project so they are not separately usable by End Users, (iii) you do not distribute in source code form Lumberyard Redistributables that we make available in file formats that are commonly compiled (e.g., C, C++) or for which we make a compiler available, and (iv) you ensure End Users are subject to terms no less protective of the Lumberyard Materials than these Service Terms, including this Section and Sections 57.4 and 57.5 below. You may sublicense these rights, subject to the restrictions in these terms, to your End Users to allow them to use, modify, create new content for, and redistribute your Lumberyard Project (e.g., create new items or levels for a game).

c. Collaboration with other AWS Customers. You may reproduce and distribute (but not sublicense) the Lumberyard Materials (including any permitted modifications and derivatives) (i) to other AWS customers that are contractors of yours solely for the purpose of allowing those AWS customers to perform work on your behalf, (ii) to other AWS customers in connection with work you perform for them as a contractor, and (iii) to up to 5 other AWS customers who you authorize to distribute a Lumberyard Project in connection with your sale or licensing of that Lumberyard Project (e.g., publishers of a game you develop). Those other AWS customers' rights to the Lumberyard Materials are governed by their agreement(s) with us.

57.3 No License Fee. There is no fee for the licenses granted in Section 57.2. Other Service Offerings and Third Party Content made available in connection with the Lumberyard Materials may be subject to separate charges and governed by additional terms.

57.4 Operating Restrictions. Without our prior written consent, (a) the Lumberyard Materials (including any permitted modifications and derivatives) may only be run on computer equipment owned and operated by you or your End Users, or on AWS Services, and may not be run on any Alternate Web Service and (b) your Lumberyard Project may not read data from or write data to any Alternate Web Service. "Alternate Web Service" means any non-AWS web service that is similar to or can act as a replacement for the services listed

[atdocs.aws.amazon.com/console/lumberyard/userguide/alternate-web-services](https://docs.aws.amazon.com/console/lumberyard/userguide/alternate-web-services) .

57.5 Other Restrictions. Without limiting the license restrictions set out in the Agreement, you may not (a) distribute the Lumberyard Materials in source code form, except as expressly permitted by Section 57.2(b) and (c), (b) use or exploit the Lumberyard Materials or any portion thereof to develop, maintain, participate in the development of, or support any competing engine, development tool, or software framework, (c) use the Lumberyard Materials or any portion thereof as part of a logo or trademark, (d) remove, obscure, or alter any proprietary rights notices (including copyright and trademark notices) contained in the Lumberyard Materials, (e) take any action that would require us or you to license, distribute, or otherwise make available to anyone the Lumberyard Materials under different terms (e.g., combining Lumberyard Materials with software subject to "copyleft" open source licenses), or (f) use or exploit

the Lumberyard Materials or any portion thereof in any manner or for any purpose other than as expressly permitted by these terms.

57.6 Registration; Release. Before distributing your Lumberyard Project to End Users, you must register it at aws.amazon.com/lumberyard/registration. You must obtain our prior written consent if the initial public or commercial release of your Lumberyard Project is based on a version of the Lumberyard Materials more than 5 years old.

57.7 Credit. You must credit us in Lumberyard Projects in accordance with the guidelines located at aws.amazon.com/lumberyard/logo-guidelines. AWS Marks included in the Lumberyard Materials may only be used in accordance with the Trademark Use Guidelines. We may use excerpts of publicly released promotional material from your Lumberyard Projects and related trademarks, service marks, trade names, and logos in connection with our marketing, advertisement, and promotion of Lumberyard.

57.8 Forums; Submissions. When discussing Lumberyard Materials in our forums or elsewhere, you may include up to 50 lines of source code from the Lumberyard Materials for the sole purpose of discussing that code. You must identify us as the source of the code. Content relating to Lumberyard Materials that you post or otherwise submit to developer discussion sites, sample code repositories, or other AWS or public forums (collectively, “Lumberyard Submissions”) constitute Your Submissions under the Agreement, and you grant (i) us a non-exclusive, worldwide, perpetual, irrevocable, transferrable, sublicensable, royalty-free, and fully paid up license under all intellectual property rights to your Lumberyard Submissions, and (ii) other AWS customers the same rights to your Lumberyard Submissions as these Service Terms provide to the Lumberyard Materials.

57.9 Data Collection. The Lumberyard Materials may provide us with information about the use of the Lumberyard Materials, including information about system and server resources, features used in the integrated development environment, frequency and duration of use, geographic and network locations, and error and information messages.

57.10 Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the [AWS Acceptable Use Policy](#). The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as use in operation of medical equipment, automated transportation systems, autonomous vehicles, aircraft or air traffic control, nuclear facilities, manned spacecraft, or military use in connection with live combat. However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.

57.11 Termination. Your rights in the Lumberyard Materials automatically terminate if the Agreement terminates or you breach the Agreement (including these Service Terms). However, if we terminate the Agreement for convenience, your rights in Lumberyard Materials then in your possession survive termination with respect to any

previously registered Lumberyard Project. Otherwise, upon termination, you must cease all use, distribution, and other exploitation of the Lumberyard Materials (and any modifications and derivatives).

58. Amazon GameLift.

58.1 Your Content. You are solely responsible for Your Content, including (a) the performance of software you use with Amazon GameLift and (b) maintaining licenses and adhering to the license terms of any software you run.

58.2 Other Services. When you use Amazon GameLift, you are also using Amazon EC2. Amazon EC2 and certain other Service Offerings and Third Party Content made available via Amazon GameLift are subject to separate charges and governed by additional terms.

58.3 Daily Active Users. Amazon GameLift fees are based in part on the number of your End Users that connect to Amazon GameLift. To allow us to accurately calculate your fees, you must provide us a unique, non-personally identifiable identifier for each of those End Users, as specified in the Amazon GameLift documentation.

58.4 Inactivity. We may delete, upon 30 days' notice to you and without liability of any kind, any of Your Content uploaded to Amazon GameLift if it has not been run for more than 3 months.

58.5 Your GameLift Data. Amazon GameLift may enable you to collect information and data from your End Users ("Your GameLift Data"). Your GameLift Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your GameLift Data, and (b) collect, use, transfer, and store Your GameLift Data in accordance with any privacy notice you provide and all applicable laws.

info|RELIANCE

STATE OF UTAH DIVISION OF PURCHASING NASPO VALUEPOINT CLOUD SOLUTIONS

SUBMITTED TO:

State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Mr. Christopher Hughes
Assistant Director
christopherhughes@utah.gov
(801) 538-3254

SUBMITTED BY:

InfoReliance Corporation
4050 Legato Road, Suite 700
Fairfax, VA 22033

Ms. Theresa Grouge
Director of Contracts
Theresa.grouge@info reliance.com
(703) 246-9360, x1162 (phone)
(703) 246-9331 (fax)

Attachment I – Draft Ordering Instructions and Template

InfoReliance is proud to have been awarded a Master Agreement from NASPO ValuePoint to provide Cloud Infrastructure as a Service (IaaS) Solutions. Our full catalog includes 53 distinct offerings from our Fulfillment Partner Amazon Web Services (AWS). Value-added services in scope under the Master Agreement include service provisioning, billing and invoicing, identity and access management, reporting, 24x7x365 Enterprise Service Desk support, and training.

Additionally, we offer optional related services including systems engineering and configuration, cloud migration, custom application development, cloud consulting, network and database administration, cloud single sign on, disaster recovery, and Big Data and analytics. These are available as established in each Participating Entity's negotiated Participating Addendum.

InfoReliance Corporation Ordering Instructions

InfoReliance Corporation Ordering Instructions	
Master Agreement Number	[TBD on award]
Contract Type	Catalog pricing with two percent (2%) minimum discount off list
Contract Duration	10 years
Authorized Buyers	All NASPO Participating Entities may negotiate a Participating Addendum under this Master Agreement.
Scope	The Master Agreement contract provides Participating Entities with access to technical capabilities that run in cloud environments and meet the NIST Essential Characteristics. All InfoReliance offerings are classified as Infrastructure as a Service (IaaS), meet the NIST definition of Cloud Computing, and are open to all deployment models (private, public, community, or hybrid).
CAGE Code	1Q4A0
DUNS Number	143147762
Federal TIN	54-1979520
Address	InfoReliance Corporation 4050 Legato Road, Suite 700 Fairfax, VA 22033
Payment Terms	Net 30 Days
Payment Information	PNC Bank Checking Account Number: 5303792351 ABA/Routing Number: 054000030
Warranty	Standard Commercial Warranty included; Extended Warranty and Customized Options Available
To obtain a quote for cloud services	naspo@infoforeliance.com
To receive policy and procedural information regarding installation, basic warranty, extended warranty, technical support, software support and other post-delivery issues	naspo@infoforeliance.com You may also contact AWS Business Support directly through your AWS account for access to AWS Cloud Support engineers.
To troubleshoot a problematic order	naspo@infoforeliance.com
Links to Related Web Sources	Sales and Ordering: https://www.infoforeliance.com/naspo AWS Calculator: http://calculator.s3.amazonaws.com/index.html AWS Product Documentation: https://aws.amazon.com/products

InfoReliance Corporation Contact Information

InfoReliance Corporation Contact Information	
Customer Service Desk	[Toll free number to be established after award] naspo@infoeliance.com
NASPO Contract Manager	Ms. Theresa Grouge 703-246-1162 (Phone) 703-246-9331 (Fax) theresa.grouge@infoeliance.com
NASPO Contract Administrator	Ms. Athena Partik 703-246-9360 x1647 athena.partik@infoeliance.com
NASPO Usage Report Administrator	Ms. Lauren Gardner 703-278-7735 lauren.gardner@infoeliance.com
Executive Sponsor	Mr. John Sankovich 703.246.9360 x1115 john.sankovich@infoeliance.com
Director of Sales Operations	Mr. Steven Johnson 703-460-2057 steven.johnson@infoeliance.com
Sales Operations Manager	Mr. Daniel Archer 703-278-7721 daniel.archer@infoeliance.com

Sample NASPO Ordering Template/Input Form

NASPO RFQ #: (if applicable use ValuePoint eMarket Center number)		
Request Date: dd/mm/yyyy	Reply By Date: dd/mm/yyyy	00:00 AM/PM ET
Subject:		
Request Type: Request For Quote		
State/Local/Education/Agency Name:	POC First Name:	
	POC Last Name:	
Fax #:	E-mail:	
Street:		
City:	State:	Zip:
NASPO Contract Holder	Contract #	
InfoReliance Corporation	TBD on award	
Attachment (if required for parts, details or scope):		
Requirements: Provide a description of products or services required with details to properly provide a quote.		