

**STATE OF UTAH COOPERATIVE CONTRACT**

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

CALIBRE Systems, Inc.

Name

CALIBRE Systems, Inc. 6354 Walker Lane, Suite 500

Street Address

Alexandria

VA

22310-3252

City

State

Zip

Vendor # VC226522 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact Name: Barbara A. Richitt Phone Number: 703-797-8500 Email: contracts@calibresys.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

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

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

5. CONTRACT PERIOD: Effective Date: Friday, April 26, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

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

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

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

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:

- a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

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

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

April 26, 2019

Contractor's signature

Date

DIVISION OF PURCHASING

Christopher Hughes (Apr 26, 2019)

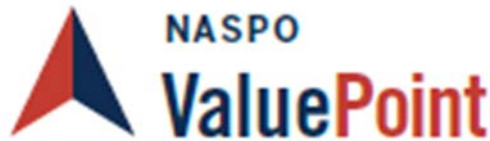
Apr 26, 2019

Director, Division of Purchasing

Date

Barbara A. Richitt, VP of Contracts & Procurement

Type or Print Name and Title



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

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

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

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

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

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the

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

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

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

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

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

13. Indemnification

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. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

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

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.

requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

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

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

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

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

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

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

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

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata. Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

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

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

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

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

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

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

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

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

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

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

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

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

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

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

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

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

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

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

37. Governing Law and Venue

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

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

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

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

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

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

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

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

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

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

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at <http://calculator.naspovaluepoint.org>. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

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

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

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

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

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

within the Participating State.

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

- a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.
- b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.
- c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.
- d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.
- e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.
- f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.
- g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

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

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	x	x	x	Private, Community, Public, Hybrid

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

2.1 Deployment Models.

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

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

Attachment C - Pricing Discounts and Schedule

Contractor: Calibre Systems, Inc.

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.
5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
SaaS Minimum Discount % * (applies to all OEMs offered within this SaaS model)	2.25%
Average SaaS OEM Discount Off	2.25%

Additional Value Added Services

Item Description	Onsite Hourly Rate		Remote Hourly Rate	
	NVP Price	Catalog Price	NVP Price	Catalog Price
Maintenance Services	N/A	N/A	N/A	N/A
Professional Services				
Deployment Services	N/A	N/A	N/A	N/A
Integration Services)	N/A	N/A	N/A	N/A
Consulting/Advisory Services	N/A	N/A	N/A	N/A
Architectural Design Services	N/A	N/A	N/A	N/A
Statement of Work Services	N/A	N/A	N/A	N/A
Partner Services	N/A	N/A	N/A	N/A
Training Deployment Services	N/A	N/A	N/A	N/A
Analysts				
Assistant Analyst	\$ 61.73	N/A	\$ 61.73	N/A
Analyst	\$ 107.76	N/A	\$ 107.76	N/A
Program Analyst	\$ 112.10	N/A	\$ 112.10	N/A
Senior Systems Analyst	\$ 123.96	N/A	\$ 123.96	N/A
Senior Analyst	\$ 128.69	N/A	\$ 128.69	N/A
Senior Program Analyst	\$ 129.71	N/A	\$ 129.71	N/A
Principal Systems Analyst	\$ 137.97	N/A	\$ 137.97	N/A
Business Analyst	\$ 153.06	N/A	\$ 153.06	N/A
Principal Analyst	\$ 159.83	N/A	\$ 159.83	N/A
Sr. Business Analyst	\$ 185.00	N/A	\$ 185.00	N/A
Consultants				
Junior Data Scientist	\$ 101.57	N/A	\$ 101.57	N/A
Junior Functional Specialist	\$ 110.00	N/A	\$ 110.00	N/A
Cloud Systems Engineer	\$ 110.04	N/A	\$ 110.04	N/A
Cloud/Web Developer	\$ 115.69	N/A	\$ 115.69	N/A
Functional Specialist	\$ 120.00	N/A	\$ 120.00	N/A
Data Scientist	\$ 129.80	N/A	\$ 129.80	N/A
Data Warehousing Applications Developer	\$ 131.34	N/A	\$ 131.34	N/A
Cloud/Web Architect	\$ 133.77	N/A	\$ 133.77	N/A
Data Warehousing Analyst	\$ 139.50	N/A	\$ 139.50	N/A
Senior Functional Specialist	\$ 146.34	N/A	\$ 146.34	N/A
Senior Cloud Systems Engineer	\$ 150.70	N/A	\$ 150.70	N/A
Senior Systems Architect	\$ 153.41	N/A	\$ 153.41	N/A
Senior Data Scientist	\$ 178.89	N/A	\$ 178.89	N/A
Senior Cloud/Web Architect	\$ 180.57	N/A	\$ 180.57	N/A
Data Mining Specialist	\$ 200.00	N/A	\$ 200.00	N/A
Consultant	\$ 206.74	N/A	\$ 206.74	N/A
Senior Consultant	\$ 209.87	N/A	\$ 209.87	N/A
Cloud Specialist (SME)	\$ 225.72	N/A	\$ 225.72	N/A
Consulting Functional Expert	\$ 245.18	N/A	\$ 245.18	N/A
SME Data Scientist	\$ 304.70	N/A	\$ 304.70	N/A

Attachment C - Pricing Discounts and Schedule

Contractor: Calibre Systems, Inc.

Database Specialists				
Junior Database Administrator	\$	80.38	N/A	\$ 80.38 N/A
Database Administrator	\$	130.78	N/A	\$ 130.78 N/A
Database Architect	\$	151.40	N/A	\$ 151.40 N/A
Senior Database Administrator	\$	159.91	N/A	\$ 159.91 N/A
Documentation Specialists				
Junior Documentation Specialist	\$	44.05	N/A	\$ 44.05 N/A
Documentation Specialist	\$	72.77	N/A	\$ 72.77 N/A
Technical Writer	\$	75.70	N/A	\$ 75.70 N/A
Senior Documentation Specialist	\$	87.37	N/A	\$ 87.37 N/A
Engineers				
Network Technician	\$	74.55	N/A	\$ 74.55 N/A
Information Engineer	\$	98.85	N/A	\$ 98.85 N/A
Network Engineer	\$	111.19	N/A	\$ 111.19 N/A
Senior Information Engineer	\$	132.43	N/A	\$ 132.43 N/A
Principal Information Engineer	\$	144.66	N/A	\$ 144.66 N/A
Senior Network Engineer	\$	155.86	N/A	\$ 155.86 N/A
Management & Business Process				
Task Leader	\$	106.50	N/A	\$ 106.50 N/A
Junior Project Manager	\$	108.00	N/A	\$ 108.00 N/A
Senior Task Leader	\$	124.13	N/A	\$ 124.13 N/A
Project Manager	\$	148.87	N/A	\$ 148.87 N/A
Senior Project Manager	\$	165.00	N/A	\$ 165.00 N/A
DevOPS Manager	\$	180.57	N/A	\$ 180.57 N/A
Program Manager	\$	193.74	N/A	\$ 193.74 N/A
Program Executive	\$	230.00	N/A	\$ 230.00 N/A
Programmers & Testers				
Junior Testing Specialist	\$	74.55	N/A	\$ 74.55 N/A
Computer Programmer/Analyst	\$	86.19	N/A	\$ 86.19 N/A
Testing Specialist	\$	110.00	N/A	\$ 110.00 N/A
Systems Programmer/Analyst	\$	113.05	N/A	\$ 113.05 N/A
Senior Programmer	\$	122.57	N/A	\$ 122.57 N/A
Senior Systems Programmer/Analyst	\$	124.53	N/A	\$ 124.53 N/A
Senior Testing Specialist	\$	142.82	N/A	\$ 142.82 N/A
Senior Programmer Analyst	\$	151.40	N/A	\$ 151.40 N/A

*NVP hourly rates listed in the above table represent rates for Calendar Year (CY) 2018.

Please see the CALIBRE Product Catalog for hourly rates for CY 2019 - 2026.

Deliverable Rates

	NVP Price	Catalog Price
Travel Reimbursement - If Needed	Cost Reimbursable	Cost Reimbursable
N/A	N/A	N/A

The logo for CALIBRE Systems, Inc. features the word "CALIBRE" in a white, sans-serif font. Above the letters "A" and "L" is a thin horizontal orange line. The logo is positioned on the left side of a large blue vertical bar that runs down the page.

**State of Utah, Division of Purchasing and
National Association of State Procurement
Officials (NASPO) ValuePoint**

**Cloud Solutions Request for Proposal (RFP)
Solicitation: SK18008**

**CALIBRE Technical Response
(RFP Section 8)**

Prepared for:

Solomon Kingston

State Contract Analyst

State of Utah, Division of Purchasing

skingston@utah.gov

(801) 538-3228

Submitted via SciQuest

July 6, 2018, 3:00 PM MT

CALIBRE Systems, Inc.

6354 Walker Lane
Metro Park, Suite 500
Alexandria, Virginia
22310-3252

p: 703.797.8500

f: 703.797.8501

www.calibresys.com

Table of Contents

TECHNICAL NARRATIVE.....	1
8 TECHNICAL REQUIREMENTS.....	4
8.1 (M)(E) TECHNICAL REQUIREMENTS.....	4
8.1.1, 8.1.2 and 8.1.3 NIST, Requirements of Attachments C & D.....	4
8.2 (E) SUBCONTRACTORS	9
8.2.1 Use of Subcontractors to Provide Cloud Solutions.....	9
8.2.2 Use of Subcontractors to Perform Contract Requirements	9
8.2.3 Qualifications of Subcontractors.....	10
8.3 (E) WORKING WITH PURCHASING ENTITIES.....	10
8.3.1 Data Breach	10
8.3.2 Pushing Adware, Software, or Marketing	12
8.3.3 User Test / Staging Environment	12
8.3.4 Americans with Disability Act	12
8.3.5 Web Browsers.....	13
8.3.6 Execution of a Service Level Agreement.....	13
8.3.7 Project Schedule Plans	14
8.3.8 Periodic Service Updates.....	15
8.4 (E) CUSTOMER SERVICE	15
8.4.1 Customer Service Standards	15
8.4.2 Customer Service Requirements	17
8.5 (E) SECURITY OF INFORMATION	20
8.5.1 Protecting Data	20
8.5.2 Complying with Data Privacy and Security Laws	21
8.5.3 Accessing Purchasing Entity's User Accounts and Data.....	22
8.6 (E) PRIVACY AND SECURITY	22
8.6.1 Compliance Programs.....	22
8.6.2 Security Certifications.....	22
8.6.3 Data Security.....	23
8.6.4 Data Confidentiality Standards.....	26
8.6.5 Third-Party Attestations.....	27
8.6.6 Logging Process	27
8.6.7 Restrict Visibility of Cloud Hosted Data	29
8.6.8 Notification Process for Security Incident.....	30
8.6.9 Isolation of Host Servers	30
8.6.10 Security Technical Reference Architectures.....	31
8.6.11 Security Procedures for Employees	32
8.6.12 Security of Confidential Data at Rest and In Transit.....	32
8.6.13 Notification of Cardholders Data Breach	33
8.7 (E) MIGRATION AND REDEPLOYMENT PLAN.....	33

8.7.1 End of Life Activities	33
8.7.2 Return of Data.....	33
8.8 (E) SERVICE OR DATA RECOVERY.....	34
8.8.1 Contingency Plan	34
8.8.2 Backup and Restore Services	35
8.9 (E) DATA PROTECTION	38
8.9.1 Standard Encryption Technologies	38
8.9.2 Business Associate Agreement.....	38
8.9.3 Use of Government Data.....	39
8.10 SERVICE LEVEL AGREEMENTS	39
8.10.1 Negotiating the Service Level Agreement	39
8.10.2 Sample Service Level Agreement.....	39
8.11 (E) DATA DISPOSAL.....	40
8.12 (E) PERFORMANCE MEASURES AND REPORTING.....	40
8.12.2 Standard Uptime Service	41
8.12.3 Support Process.....	41
8.12.4 SLA Remedies – Incident Response Time.....	41
8.12.5 Planned Downtime	41
8.12.6 SLA Remedies – Disaster Recovery	42
8.12.7 Sample of Performance Reports	42
8.12.8 Ability to Print Historical, Statistical, and Usage Reports.....	44
8.12.9 24x365 On-Demand Deployment.....	44
8.12.10 Scale-up and Scale-down	45
8.13 (E) CLOUD SECURITY ALLIANCE	46
8.14 (E) SERVICE PROVISIONING	47
8.14.1 Emergency or Rush Services Implementation Process.....	47
8.14.2 Standard Lead-time for Provisioning Solutions	47
8.15 (E) BACK UP AND DISASTER PLAN.....	48
8.15.1 Legal Retention Periods.....	48
8.15.2 Known Inherent Disaster Recovery Risks	48
8.15.3 Infrastructure Support for Multiple Data Centers within the United States	48
8.16 (E) HOSTING AND PROVISIONING	50
8.17.1 Cloud Hosting Provisioning Processes.....	50
8.17.2 Tool Sets	51
8.17 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE).....	54
8.18.1 Testing and Training Periods	54
8.18.2 Test and/or Proof of Concept Environment	54
8.18.3 Training and Support at No Cost.....	54

8.18 E) INTEGRATION AND CUSTOMIZATION	54
8.19.1 Integrated Solutions	54
8.19.2 Customized and personalized Solutions	55
8.19 (E) MARKETING PLAN	55
8.20 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS	56
8.22 (E) SUPPORTING INFRASTRUCTURE	56
8.22.1 Solution Infrastructure	56
8.22.2 Installation of New Infrastructure	56

List of Tables

Table 1: Level of Data Risk per Service Model.	6
Table 2: AWS Support Features.....	18

List of Figures

Figure 1: The CALIBRE VAPOR™ Methodology.....	2
Figure 2: CALIBRE Escalation Path.....	17
Figure 3: AWS Shared Responsibility Model.....	21
Figure 4: AWS Isolation and Deployment	31
Figure 5: AWS Enterprise Security Architecture	32
Figure 6: Regions and Availability Zones	36
Figure 7: Global Map of AWS Regions and Availability Zones.....	37
Figure 8: Sample AWS Reports.....	44
Figure 9: Amazon CloudWatch	46

TECHNICAL NARRATIVE

3.10 SUBMISSION OF PROPOSAL; 5 Section title: Technical Response. This section should constitute the Technical response of the proposal and must contain at least the following information:

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

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

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

CALIBRE's solution offers the State of Utah, Division of Purchasing, NASPO, and their clients with the leading cloud provider, Amazon Web Services, Inc. (AWS), paired with CALIBRE's experience and skills as a proven system integrator. CALIBRE's offerings span the entire suite of AWS products for solutions in all three of the service areas: Infrastructure as a Service (IaaS), Platform as a Service (IaaS), and Software as a Service (SaaS). CALIBRE is an AWS partner with trained and certified staff who have experience implementing systems for Government and education clients. CALIBRE has been providing cloud solutions for over 10 years, including large scale projects for the University of Hawaii, National Institutes of Health, Department of Homeland Security, Eli Lilly, Memorial Healthcare Services, Federal Energy Regulatory Commission, and several organizations within the Department of Defense. We provide these services under contract vehicles similar to NASPO, including the Army Cloud Computing Enterprise Transformation (ACCENT), General Services Administration (GSA) IT Schedule 70, Army Training Support Systems-Enterprise (TSS-E), and State of Maryland Consulting and Technical Services Plus.

AWS is the most recognizable and widely used cloud service provider in the United States and throughout the world. Gartner describes AWS as "the dominant market leader and an IT thought leader for more than 10 years, not only in IaaS, but also in integrated IaaS+PaaS." Gartner has assessed them as the most mature cloud provider available. They continue to assert that AWS "is the provider not only chosen by clients that value innovation and are implementing digital business projects, but also preferred by clients that are migrating traditional data centers to cloud IaaS. It can readily support mission-critical production applications, as well as the implementation of highly secure and compliant solutions." Gartner's independent review and analysis of AWS points to their standing and qualifications as the leading cloud services provider to support NASPO ValuePoint Cloud Master Agreement.

As a recognized industry leader AWS provides flexible, cost effective, scalable, innovative, and secure cloud services and solutions. AWS continually expands its services to support virtually any cloud workload. AWS now has more than 100 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid, and enterprise applications.

CALIBRE's relationship with AWS includes highly knowledgeable liaisons and points of contacts who work directly with our Contract Manager and technical leads so that AWS Service Level Agreements (SLAs), performance monitoring, and issue resolution are compliant with this

master agreement and any subsequent statements of work. Through our technical workforce in coordination with our Contract Manager, CALIBRE will continuously conduct oversight and performance validation throughout our service and support to NASPO ValuePoint participants.

CALIBRE uses our trademarked VAPOR™ approach when providing services. We **Validate** system architecture and associated servers, **Analyze** data for migration, **Plan** the migration and integration, **Orchestrate** our plan to execution, and allow agencies to **Realize** the benefits of their move to the cloud. VAPOR incorporates best practices and lessons learned from years of providing cloud services, minimizing risk while migrating to the cloud. Using this approach, we provide cloud migrations and managed services, application development, security services, and more specialized cloud offerings. The VAPOR approach shown in Figure 1 provides a structured framework to address the migration of applications to the cloud.



Figure 1: The CALIBRE VAPOR™ Methodology - The key to Successful Cloud Modernization and Transition.

CALIBRE used VAPOR for the migration of several systems from on-premise to cloud solutions for both Defense and Civilian projects, like the Army Meter Data Management System's (MDMS) migration to Defense Information Systems Agency (DISA) MilCloud; the Logistics Integrated Warehouse – Integrated Logistics Analysis Program (LIW-ILAP) to a military-run enterprise data center; and the Federal Energy Regulatory Commission's (FERC) eLibrary modernization into AWS. VAPOR is a phased approach representative of the efforts required to

first modernize an application to leverage the cloud capabilities and then perform the transition to the new environment. The VAPOR methodology contains five steps, including:

- ▶ **Validate** through a review of the application documentation for topics such as incorporated technologies, data structures and sharing, external interfaces, and dependencies and components. A firm baseline of the application as it exists is a key factor to determining the actions necessary for a modernization and cloud migration effort. Legacy systems often have out-of-date or minimal documentation so an extensive effort may be necessary to perform this validation.
- ▶ **Analyze** the validated documentation to develop alternative analyses and establish initial discussions with the other organizations impacted by the cloud transition. The analysis focuses on areas where modernization can fully leverage the benefits of the cloud infrastructure while improving the application stance for areas such as security, performance, recoverability, scalability, and maintainability. CALIBRE reviews the data structures and external interfaces to determine what the current interactions are with other systems while examining opportunities for improvement and cloud migration preparation.
- ▶ **Plan** uses the output from the previous steps to build out the target architecture, and develop a Work Breakdown Structure and overall schedule for cross-system and team coordination. Most systems will require modifications to continue interacting with other systems as external interfaces change, move, and/or modernize. In addition, the various operations, tests, and security teams have many activities to perform as they establish new environments, upload security artifacts, and modify network connections. Obtaining a commitment to the plan from all parties is a key success factor.
- ▶ **Orchestrate** the activities on the plan as a modernization and transition involves a significant number of parties with dependencies on each other. Delays can have ripple effects across the schedule. The cloud transition is most likely dependent on other systems completing their related updates to address new or changed system interfaces and network locations. Training and other management activities address user interface impacts.
- ▶ **Realize** the benefits of the cloud migration and generate the data to document the gains. The cloud environment provides a standardized mechanism to gather a wide variety of statistics to analyze performance, identify areas for additional improvement, and proactively respond to system issues.

CALIBRE will provide cloud service offerings through the use of our partnership with AWS. For any implementation or support requirements, CALIBRE will work with prospective clients to identify the most effective solution possible, many times providing direct access to our partner resources. As provided in the following sections, are the details of how CALIBRE and AWS meet the requirements of the RFP as well as the description of how CALIBRE will leverage AWS to support our clients. CALIBRE's experience with Government or large consortium contracts similar to the Master Agreements sought through this RFP and our partnership with AWS, the leading cloud services provider, provides a low risk option for successful cloud implementations.

8 TECHNICAL REQUIREMENTS

8.1 (M)(E) TECHNICAL REQUIREMENTS

8.1.1, 8.1.2 and 8.1.3 NIST, Requirements of Attachments C & D

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

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

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

CALIBRE's proposed offering meets all the fundamental cloud requirements. As described below, our solution paired with AWS offerings, fully meets the National Institute of Standards and Technology (NIST) standard. CALIBRE provides the essential services to transform these cloud characteristics into dynamic, responsive, secure, and compliant solutions. Our trained and experienced staff have the expertise to reduce deployment times and provide the functional environments that meet the Purchasing Entities needs and requirements.

Essential Characteristics

According to the official NIST definition defined in NIST Special Publication 800-145, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies. It also provides a baseline for discussion from what is cloud computing to how to best use cloud computing. The following sections detail how AWS offerings meets the NIST definition of cloud.

On-Demand Self-Service: AWS provides clients of all sizes with on-demand access to a wide range of cloud infrastructure services, charging clients only for the resources they use. AWS enables users to eliminate the need for costly hardware and the administrative challenges of owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our clients can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it easy for clients to get started and be productive.

Broad Network Access: AWS provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while clients provision and use what they need via a web application.

Resource Pooling: 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 client from other clients. AWS designed their systems to prevent clients from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. An independent PCI Qualified Security Assessor validated this architecture and found that it complied with all requirements of PCI DSS Security Standards 3.2 as of July 2016.

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

Measured Service: AWS uses automated monitoring systems to provide a high-level of service performance and availability. Proactive monitoring is available through a variety of online tools for internal and external use. AWS instrumented systems extensively to monitor key operational metrics. Alarms automatically notify operations and management personnel when early warning thresholds on key operational metrics are crossed. AWS uses an on-call schedule so personnel are available to respond to operational issues. This includes a pager system to communicate alarms quickly and reliably to operations personnel.

Cloud Service Models

The NIST definitions include three cloud service models that AWS addresses through their various products:

Infrastructure as a Service (IaaS): IaaS addresses the needs for basic infrastructure (processing, storage, networks, and other fundamental computing resources) before loading any operating systems or software. AWS provides a full suite of products including servers and storage such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Block Store (Amazon EBS).

Platform as a Service (PaaS): PaaS provides computing resources with basic services to load additional software or configure resources to establish the operational environment for an implementation. AWS provides a wide variety of capabilities for PaaS, such as AWS Directory Services, AWS RedShift for data warehousing, and Amazon Relational Database Service (RDS) with a variety of database choices (Amazon Aurora, MySQL, Oracle, Microsoft SQL Server 2016, PostgreSQL, and MariaDB).

Software as a Service (SaaS): SaaS establishes complete software packages and applications for consumer use with minimal effort. The users are usually limited to configuration settings and are not responsible for the underlying components. Examples of SaaS solutions available through AWS, include AWS QuickSight for business intelligence, WorkSpace for virtual desktops, and WorkDocs for collaborative file sharing.

Categorization of Risk

The NIST 800-53 security controls are generally applicable to Federal Information Systems. These are typically systems that must go through a formal assessment and authorization process. This is to provide sufficient protection of confidentiality, integrity, and availability of

information and information systems based on the security category, impact level of the system (low, moderate, or high), and risk determination. Table 1 below uses the Federal Risk and Authorization Management Program (FedRAMP) definitions of low, moderate (East/West) and high (GovCloud) with the approved and in-process services for each service model.

Table 1: Level of Data Risk per Service Model.

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS	▶ QuickSight ▶ AWS Config ▶ CloudTrail ▶ Cognito ▶ Key Management Service ▶ Kinesis ▶ SWF ▶ WorkDocs ▶ WorkSpaces	▶ QuickSight ▶ AWS Config ▶ CloudTrail ▶ Cognito ▶ Key Management Service ▶ Kinesis ▶ SWF ▶ WorkDocs ▶ WorkSpaces	▶ AWS Config ▶ CloudTrail ▶ Key Management Service ▶ Kinesis ▶ SWF	Public, Community or Hybrid Model
IaaS	▶ Direct Connect ▶ EC2 ▶ Elastic Block Store ▶ Glacier ▶ S3 ▶ VPC ▶ Web Application Firewall	▶ Direct Connect ▶ EC2 ▶ Elastic Block Store ▶ Glacier ▶ S3 ▶ VPC ▶ Web Application Firewall	▶ Direct Connect ▶ EC2 ▶ Elastic Block Store ▶ Glacier ▶ S3 ▶ VPC	Public, Community or Hybrid Model
PaaS	▶ CloudFront ▶ Directory Service ▶ DynamoDB ▶ Elastic Load Balancing ▶ Elastic Map Reduce ▶ ElastiCache ▶ Lambda ▶ RDS ▶ Redshift ▶ Route 53 ▶ Snowball ▶ SNS ▶ SQS	▶ CloudFront ▶ Directory Service ▶ DynamoDB ▶ Elastic Load Balancing ▶ Elastic Map Reduce ▶ ElastiCache ▶ Lambda ▶ RDS ▶ Redshift ▶ Route 53 ▶ Snowball ▶ SNS ▶ SQS	▶ DynamoDB ▶ Elastic Load Balancing ▶ Elastic Map Reduce ▶ ElastiCache ▶ Lambda ▶ RDS ▶ Redshift ▶ Snowball ▶ SNS ▶ SQS	Public, Community or Hybrid Model
Tools and supporting products not currently rated for data risk under the AWS FedRAMP certification:				
▶ Elastic File System ▶ Import/ Export ▶ Storage Gateway ▶ Data Pipeline ▶ Data Transfer		▶ SimpleDB ▶ AppStream ▶ CloudHSM ▶ CloudSearch ▶ CloudWatch		▶ Elastic Transcoder ▶ Machine Learning ▶ Mobile Analytics ▶ CodeStar ▶ CodeCommit

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
► SES		► Code Deploy		► CodePipeline ► CodeBuild

Third-party testing performed against the NIST 800-53 Revision 4 controls plus FedRAMP requirements validated AWS' NIST compliant cloud infrastructure services. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for the AWS GovCloud (US) Region and the AWS US East/West regions. AWS' whitepaper *NIST Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud* evaluates the NIST CSF and the many AWS Cloud offerings public and commercial sector clients can use to align to the NIST CSF to improve their cybersecurity posture. AWS also provides a third-party auditor letter validating attestation confirming their services' conformance to the NIST CSF risk management practices, allowing users to properly protect their data across AWS.

As users build NIST compliant AWS systems and applications, controls are the responsibility of AWS-only, clients-only, or shared between both. Under a Non-disclosure Agreement, AWS will provide an AWS FedRAMP SSP template based upon NIST 800-53 Revision 4, which is prepopulated with the applicable NIST 800-5 Rev. 4 low/moderate/high control baseline. Control responsibility is as follows:

- **Shared Responsibility** - Users provide security and configurations of their software components and AWS will provide security for its infrastructure.
- **Client-Only Responsibility** - Users are fully responsible for guest operating systems, deployed applications, and select networking resources, such as firewalls. Users are solely responsible for configuring and managing security "in" the cloud.
- **AWS-Only Responsibility** - AWS manages the cloud infrastructure, including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software. Applications built on top of the AWS system inherit the features and configurable options that AWS provides. AWS is solely responsible for configuring and managing security of the cloud.

For security authorization purposes, compliance with the FedRAMP requirements (based on NIST 800-53 Revision 4 Low/Moderate/High control baseline) is contingent upon AWS fully implementing AWS-Only and Shared controls, and the users implementing Client-Only and Shared controls. A FedRAMP accredited 3PAO (Third-Party Assessor Organization) assessed and authorized AWS' implementation of their control responsibility. The user must be separately assessing and authorizing the portion of shared controls and controls related to applications they implement on top of the AWS infrastructure.

Deployment Models

Public Model: The public model is most commonly associated with the cloud where clients share resources for the most effective use of them and for the lowest price possible. These economies of scale enable AWS to continually lower prices and deploy new services to further the adoption of the cloud. AWS cloud is openly available and AWS provides the mechanisms to completely isolate each client's operation, data, applications, and users from the other cloud clients. CALIBRE provides our VAPOR model to evaluate application readiness for the cloud and then efficiently perform migrations.

Hybrid Model (Extend IT Services): A hybrid cloud environment allows organizations to address immediate IT needs though using the benefits of cloud computing, while also retaining on-premises infrastructure. A hybrid model is a sensible approach to cloud adoption for clients that require the immediate use of scalable cloud services, but are not ready to migrate all applications and workloads to the cloud.

AWS provides the tools and solutions to integrate existing on-premises resources with the AWS cloud. By using AWS to enhance and extend user capabilities, without giving up the investments users have already made, they can accelerate their adoption of cloud computing. Some common requirements and issues associated with hybrid cloud include:

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

AWS provides the capabilities required for a dynamic, reliable, and secure hybrid cloud solution, to include:

- ▶ **Extend Network Configuration** - Flexible network connectivity is a cornerstone of integrating distributed environments, including AWS and users' existing on-premises equipment. With Amazon Virtual Private Cloud (VPC), users can extend their on-premises network configuration into their virtual private networks on the AWS cloud. AWS resources can operate as if they are part of the user's existing corporate network. Amazon VPC lets clients provision a logically isolated section of the AWS Cloud where they launch AWS resources in a virtual network that they define. Users have complete control over their virtual networking environment, including selecting their own Internet Provider (IP) address range, creation of subnets, and configuration of route tables and network gateways.
- ▶ **Integrated Cloud Backups** - AWS simplifies the backup and recovery environment for the enterprise. Users leverage the on-demand nature of the cloud and automate their backup and recovery processes so they are not only less complex and lightweight, but also easy to manage and maintain. AWS designed storage services to provide 99.99999999% durability, so users feel confident about the protection of their backups.
- ▶ **Integrated Network Connection** - AWS Storage Gateway is the best way to establish an on-premises connection with AWS. An appliance installed in users' data center with cloud-based storage, AWS Storage Gateway provides seamless and secure integration between an organization's existing IT environment and the AWS storage infrastructure. Using industry-standard storage protocols, the service allows clients to store data in the AWS cloud for scalable and cost effective storage. It provides low-latency performance by maintaining frequently accessed data on-premises while securely storing encrypted user data in the Amazon Simple Storage Service (Amazon S3), or Amazon Glacier.
- ▶ **Integrated Resource Management and Workload Migration** - Robust Application Programming Interfaces (APIs) drive AWS cloud services. APIs that allow for a wide variety of monitoring and management tools that integrate easily with client's AWS cloud

resources. Organizations can extend many of the tools they use to manage their on-premises environments to the AWS environments. Integrating clients' tools with the AWS environment provides a simpler and quicker path for cloud adoption, because their operations team does not need to learn new tools or develop completely new processes.

Solution Use Cases for AWS hybrid clouds include:

- ▶ Migrating workloads and data that are "cloud ready", such as applications that do not need significant re-architecting for a cloud migration
- ▶ Retaining data on-premises at the Purchasing Entity to meet regulatory and compliance needs

AWS provides Hybrid Cloud Resources, the tools, information, and guidance, to build a hybrid cloud environment that offers an immediate impact to clients. CALIBRE stands ready to assist clients with getting started with determining resource requirements and making them available.

8.2 (E) SUBCONTRACTORS

8.2.1 Use of Subcontractors to Provide Cloud Solutions

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.

As discussed in the Technical Narrative, CALIBRE will provide cloud service offerings through the use of our partnership with AWS. As a recognized industry leader AWS provides flexible, cost effective, scalable, and innovative, and secure cloud services and solutions with unrivaled experience. CALIBRE has been a Standard partner with AWS since 2014. For any implementation or support requirements, CALIBRE will work with prospective clients to identify the most effective solution possible, many times providing direct access to our partner resources. AWS is fully aware of and meets all administrative, business, and technical requirements of the NASPO ValuePoint Master Agreement for Cloud Solutions.

8.2.2 Use of Subcontractors to Perform Contract Requirements

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.

CALIBRE will contract AWS for providing SaaS, IaaS, and PaaS service offerings as detailed in the RFP. We will work to add value-added services and partners as they become available and as CALIBRE fully vets them. CALIBRE will employ AWS under the Master Agreement terms and conditions. CALIBRE will act as the liaison to provide seamless support and implementation throughout the lifecycle of this contract. We do not intend to use AWS personnel in any position to support potential clients. AWS will be the SaaS, IaaS, and PaaS cloud service provider.

8.2.3 Qualifications of Subcontractors

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.

AWS is the most recognizable and widely used cloud service provider in the United States and throughout the world. Gartner describes AWS as “the dominant market leader and an IT thought leader for more than 10 years, not only in IaaS, but also in integrated IaaS+PaaS,” and has assessed them as the most mature cloud provider available. Gartner continues to assert that AWS “is the provider not only chosen by clients that value innovation and are implementing digital business projects, but also preferred by clients that are migrating traditional data centers to cloud IaaS. It can readily support mission-critical production applications, as well as the implementation of highly secure and compliant solutions.” Gartner’s independent review and analysis of AWS points to their standing and qualifications as the leading cloud services provider to support NASPO ValuePoint Master Agreement for Cloud Solutions.

Our relationship with AWS includes highly knowledgeable liaisons and points of contacts who work directly with our Contract Manager and technical leads so that AWS SLAs, performance monitoring, and issue resolution are compliant with this master agreement and any subsequent statements of work. Through our technical workforce in coordination with our Contract Manager, CALIBRE will continuously conduct oversight and performance validation throughout our service and support to NASPO ValuePoint participants.

8.3 (E) WORKING WITH PURCHASING ENTITIES

8.3.1 Data Breach

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.***

As AWS is a platform, CALIBRE maintains control of content on the platform under the direction and on behalf of the Purchasing Entities. CALIBRE engineers will monitor the environment within an Amazon VPC for data breaches and then notify CALIBRE’s Contract Manager and assigned Points of Contact for the Purchasing Entity. The Purchasing Entity is also responsible for notifying CALIBRE if unusual patterns or activity is identified on their environment.

AWS services are content agnostic, in that they offer the same high-level of security to clients, regardless of the type of stored content, or the geographical region in which they store their content. Purchasing Entities retain ownership and control of their content when using AWS services and CALIBRE administers the content and services on behalf of the Purchasing Entities. CALIBRE will work with the Purchasing Entities to determine what content they store or

process using AWS services along with determining what level of security is appropriate. In the event of a privacy breach, CALIBRE will work with the Purchasing Entity and follow their directions to notify regulators and affected individuals as required under applicable law. CALIBRE will work with each Purchasing Entity to establish the appropriate notification processes.

CALIBRE will implement a formal, documented incident response policy and program for each Purchasing Entity based on our existing program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. Below is an outline of the four-phased approach to manage data breach incidents:

- 1) **Activation and Internal Notification Phase** - Incidents begin with the detection of an event and the Purchasing Entity notification will occur upon validation of the breach. This event identification can come from several sources including:
 - a. Metrics and Alarms – AWS maintains a robust situational awareness capability that CALIBRE uses for system monitoring. AWS also uses early indicator alarms to proactively identify issues that may ultimately impact their clients. AWS rapidly detects the majority of issues from 24x7x365 monitoring and alarming of real-time metrics and service dashboards. CALIBRE will monitor and address the issues raised through these mechanisms.
 - b. Trouble Ticket - A Purchasing Entity enters or calls in a Support Ticket that identifies a potential breach.
- 2) **Recovery Phase** – Resolvers will perform break fix to address incidents. The resolvers are AWS and/or CALIBRE employees depending on the root cause. Once they address troubleshooting, break fix, and the affected components, the assigned CALIBRE employee will determine next steps in terms of follow up documentation and actions. The timeline is dependent on the incident so CALIBRE will continually communicate resolution timelines to the Purchasing Entity during the recovery phase.
- 3) **External Notification Phase** – Upon completion of the recovery, CALIBRE will work with the Purchasing Entity to perform the required notifications. The CALIBRE Contract Manager will work on the processes and timelines with their designated contact.
- 4) **Reconstitution Phase** – Once the relevant fix activities are complete the assigned AWS employee will declare that the recovery phase is complete. AWS will assign the post mortem and deep-root-cause analysis of incident to the relevant team. AWS senior management will review the results of the assigned and post mortem and actions. This includes the review of design changes and Correction of Errors (COE) to verify that AWS employees documented and tracked them to completion. After the AWS team completes the incident resolution, they perform a root cause analysis the next business day.

In addition to the internal communication mechanisms detailed above, AWS also has various methods of external communication to support its client base and community. Mechanisms notify the CALIBRE team of operational issues that impact the Purchasing Entity experience. AWS maintains a "Service Health Dashboard" (<http://status.aws.amazon.com/>) that alerts CALIBRE to any issues of broad impact. CALIBRE leverages these communications channels to monitor and respond to alerts on behalf of the Purchasing Entities. CALIBRE's cloud

engineers evaluate the alerts, determine necessary course of action for our clients, communicates impacts and potential actions to the Purchasing Entity's technical contacts, and then CALIBRE executes the agreed upon plan of action.

Independent external auditors review the AWS incident management program and audits for System and Organization Controls (SOC), PCI DSS, ISO 27001, and FedRAMP compliance. Additionally, AWS maintains and updates their incident response playbooks to reflect emerging risks and lessons learned from past incidents. AWS tests the plans and makes updates through the due course of business (at least monthly).

8.3.2 Pushing Adware, Software, or Marketing

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.

CALIBRE certifies that we, and our partner AWS, will not engage in, or permit agents to push adware, software, or marketing not authorized by the Participating Entity or the Master Agreement. There is a possibility that a Purchasing Entity may engage in activities that cause unintended pushes of such items that are out of the control of CALIBRE and our vendor. CALIBRE will work with Participating Entities to identify and understand those items that are at their sole control. Our Contracts Manager will acquire software through authorized purchase / acquisition orders.

8.3.3 User Test / Staging Environment

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

CALIBRE follows industry best practices in establishing a user test/staging environment that directly matches the production environment. Our development and deployment process generally uses four environments: Development, Testing, Staging, and Production (along with applicable disaster recovery capabilities). CALIBRE first develops or implements code and system changes in the lower environments (Dev and Test) for validation and promotion into Staging. As a replica of Production, Staging provides an opportunity to perform full functional, load and performance, and acceptance testing using the full set of deployment scripts. AWS tools and capabilities support these processes to permit automation and testing for a test / staging environment that matches production.

8.3.4 Americans with Disability Act

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

In 1998, the U.S. Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. Congress enacted Section 508 to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies to achieve these goals.

The law applies to Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. ' 794d), agencies must give disabled

employees and members of the public access to information that is comparable to the access available to others.

CALIBRE provides software development and support services to numerous Federal Government agencies with 508 compliance requirements. For example, the Department of Homeland Security (DHS) established training and certification requirements for 508 testers. CALIBRE's testing staff completed the certification process on these DHS contracts. Our deep experience and understanding of Federal 508 compliance directly translates into capabilities that are applicable for AWS hosted applications.

The AWS ElasticWolf Client Console incorporates Section 508 requirements. AWS also has a Voluntary Product Accessibility Template (VPAT) for the Console that outlines the Console's accessibility features. AWS offers the VPAT upon request.

AWS provides API-based cloud computing services with multiple interfaces to those services, including Software Development Kits (SDKs), Integrated Development Environment (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.

8.3.5 Web Browsers

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 a minimum

AWS applications, products, and capabilities are accessible through web browsers. The supported browsers vary by individual application and AWS lists the supported browsers on their website. As an example of how AWS approaches browser support, AWS supports the following browsers for the AWS Management Console:

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

8.3.6 Execution of a Service Level Agreement

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Before the execution of a SLA, CALIBRE will meet with the Purchasing Entity to fully document and understand the full set of requirements and identify risks and potential issues. Upon an order or award, our Contracts Manager will assign a Project Manager, and other needed subject matter experts, to schedule a kickoff meeting with Contracting Officer's identified stakeholders. The primary goals of holding a kickoff meeting is to establish a strong professional relationship for efficient and effective communication and support through the life

of support. During the meeting CALIBRE will work with stakeholders to define roles and responsibilities, schedules, major milestones, communication procedures, and provide an understanding of resources required to accomplish the work. CALIBRE will tailor each kickoff meeting to meet the client's requirements set forth in the order or award. CALIBRE's analysts will work with the Purchasing Entity to evaluate and categorized the data being stored as Personally Identifiable Information (PII), Protected Health Information (PHI) or other types of sensitivity. CALIBRE's Contracts Manager and Project Manager will work with the participating entity to determine the mechanisms and approaches to protect sensitive or personal information in accordance with appropriate rules, regulations and guidance. We will establish procedures for safeguarding, handling, and storing such information. CALIBRE will follow the appropriate guidance from AWS for specific situations such as HIPAA compliance.

CALIBRE regularly works with sensitive information and has a Top Secret facility clearance and is authorized secure storage at the Secret level. Our over 800 employees include approximately 630 who have some form of clearance from Public Trust to Top Secret Sensitive Compartmented Information (TS/SCI) with a polygraph. Over 420 employees have access to Secret or Top Secret information. These employees go through annual refresher training to protect sensitive, classified and/or personal information.

CALIBRE employees also regularly protect Personal Identifiable Information (PII), business sensitive information, and company propriety information. Most of our classified contracts are with Federal agencies and the Department of Defense. CALIBRE also has a large healthcare Information Technology market set of contracts at the National Institutes of Health (NIH) where we work with 20 of the 27 agencies. We work with PII, including Health Insurance Portability and Accountability Act data on a daily basis.

During the last Security Vulnerability Assessment by Defense Security Service, CALIBRE achieved a Superior rating. The rating demonstrates exceptional knowledge and performance, reserved only for security programs in the top 10% of cleared industry. In addition, CALIBRE's /Facility Security Office is a board-certified Industrial Security Professional (ISP®). This brings quantified credentials and recognition as a qualified professional with knowledge, skills, and abilities above and beyond those demanded by the Security Profession.

8.3.7 Project Schedule Plans

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

An integral part of the kickoff meeting is to establish with the stakeholders an initial high-level project schedule and associated work plans. CALIBRE will use our tested Project Management Planning tools to establish and set effective schedules using widely available software tools such as Microsoft Project and SharePoint. CALIBRE suggests using Agile methodologies the development, testing, and implementation phases to gain user input throughout the life of the project. To meet the requirements of each participating entity, CALIBRE will develop schedules and plans tailored to a problem set identified during the kickoff meeting. In most cases, CALIBRE uses an Agile approach to solution development and implementation using two week sprints. We allot the first two weeks of a project for kickoff and initial requirements elicitation and verification. Next, we typically have a two week Sprint 0 to establish the infrastructure and initial architecture. Iterative two week sprints then follow a typical Scrum cycle that includes

testing. The number of sprints depends on the scope of the effort. However, we use the final two week sprint for training, user acceptance testing, and deployment support. CALIBRE also implements projects in waterfall and other methodologies depending on the needs of the Purchasing Entity.

8.3.8 Periodic Service Updates

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

- *How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.*
- *How Offeror will maintain discounts at the levels set forth in the contract.*
- *How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.*
- *How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.*

Service Line Additions and Updates pursuant to section 2.12: CALIBRE will add new AWS services to our catalog as the products are available. AWS is actively and continually developing and releasing new products that leverage the capabilities of the cloud for new solutions. CALIBRE will provide these services to meet the terms and conditions outlined in the Master Agreement and in our renewal response(s).

Maintaining discounts at the levels set forth in the contract: CALIBRE will provide the same minimum discount as set forth for the initial product list with new products added to the AWS portfolio.

Reporting to Purchasing Entities, as needed, regarding technology changes and make recommendations for service updates: CALIBRE will maintain an active relationship with our Purchasing Entities to report changes in technology and make recommendations for service updates. Our technical staff continually monitors the AWS website and product releases for new capabilities and services that improve the operations of our clients. CALIBRE will provide detailed analysis of the technology change, potential benefits, risks, and deployment activities for consideration by each of the impacted Purchasing Entities.

Transition support to any Purchasing Entity: In the unlikely event a service change may negatively impact a Purchasing Entity, CALIBRE will prepare an alternatives analysis that explains the change, impacts, and alternative options for replacing or customizing the service.

8.4 (E) CUSTOMER SERVICE

8.4.1 Customer Service Standards

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

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

Quality Assurance Measures: CALIBRE based its project management lifecycle processes on standards established by the International Organization for Standardization (ISO), the Capability

Maturity Model Integration (CMMI) Institute, and the Project Management Institute for reliable, repeatable, and best-in-class quality and project management. CALIBRE is rated at CMMI Maturity Level 2 and Capability Level 3 in several process areas to include project planning, project monitoring and control, requirements management, requirements/configuration management, process and project quality assurance. CALIBRE is also rated at CMMI Maturity Level 3 for software development. Through our internal audits and peer review process, which is a part of our overall quality management program, we continuously maintain proven, reliable, and credible project management standards on our client projects.

CALIBRE's ISO 20000-1 IT Services Certification enables reduced incident response times and interruptions to IT services; improved incident management, consistency in service delivery, and client satisfaction; greater understanding of roles and business objectives; and a culture of continuous process improvement.

A Quality Assurance Surveillance Plan (QASP) is essential for CALIBRE to deliver the purchased services on-time, on-schedule, and with the quality required under the NASPO program. Key elements of the QASP are:

- ▶ **Quality Assurance Measures** – Performance requirements define the items for review.
- ▶ **Performance Standards** – Is the level of expected activity or plan to meet the Performance Requirement.
- ▶ **Acceptable Quality Levels** – Is the metric to determine if performance exceeds, meets, or does not meet a given standard.
- ▶ **Methods of Surveillance** – Are the methods used in the administration of the QASP, which we further develop during project planning, to include:
 - Client Feedback – CALIBRE will obtain feedback either from the results of our annual client satisfaction surveys, or from random compliments or complaints we receive.
 - 100% Inspection – We accomplish 100% inspection by monitoring and documenting our processes procedures and results. Each month, the Purchasing Entities will review the CALIBRE generated documentation and enter summary results into the Surveillance Activity Checklist.
 - Periodic Inspection – The Purchasing Entities can conduct periodic inspections for identified tasks in this QASP. The appropriate Purchasing Entities' personnel typically perform the periodic monthly inspection.
 - Random Monitoring – The appropriate designated Technical Monitor conducts random monitoring for QASP compliance.

Once CALIBRE and stakeholders plan the details of the project, CALIBRE will create a QASP tailored to the client's needs.

Escalation Plan: The CALIBRE Issue Resolution Process, with escalation path, is a process we implement across all projects. The process identifies and resolves the action items, problems, and complaints quickly and to our clients' satisfaction.

CALIBRE will use Atlassian JIRA to enter, monitor, and track action items, problems, and complaints identified by NASPO and the Purchasing Entities. This tracking system allows the client to enter, review, monitor, and prioritize open items for the project. CALIBRE employs

different strategies for issue resolution based on the type of item. CALIBRE tracks and updates action items, problems, and complaints during each internal and client meeting.

For issues requiring corrective actions, the CALIBRE Project Manager will work with the Purchasing Entity's Project Manager to determine the scope of the problem, potential solution, and target timeframe. If the Purchasing Entity Project Manager and CALIBRE's Project Manager cannot reach a resolution or agreement on these items, or miss a target timeframe, CALIBRE's Project Manager will escalate the issue(s) to CALIBRE's Program Manager and Vice President (VP) responsible for the contract work. CALIBRE's VP and Program Manager will review the issue for problem resolution. If they are unable to resolve the issue with the Purchasing Entity, they will notify the NASPO Cooperative Development Team for intervention and problem resolution. The CALIBRE VP will monitor the progress towards resolution on a daily basis for the escalated items. Figure 2 shows CALIBRE's Escalation Path.

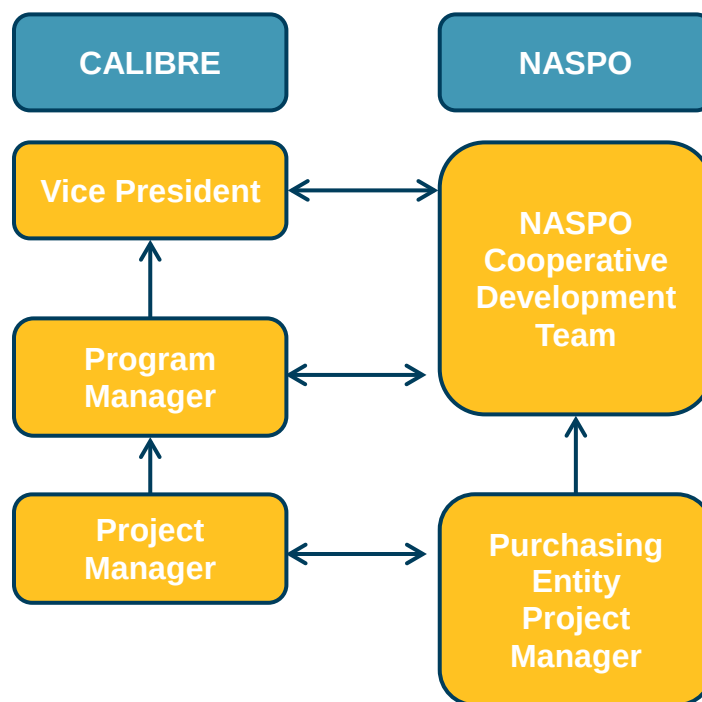


Figure 2: CALIBRE Escalation Path - A clear process for monitoring and escalating issues to the appropriate levels within NASPO and CALIBRE that is completely transparent to all parties and speeds the resolution of program and project issues.

Service Level Agreement (SLA): The SLAs CALIBRE provides, through our AWS partner, to Purchasing Entities will be reliant on the overarching solution the purchasing entity request to deploy. CALIBRE will provide AWS' SLAs, the underlying infrastructure provider, to Purchasing Entities based on the region and product set the Purchasing Entity determines, with CALIBRE's support, to best support their requirements. CALIBRE has included samples of applicable AWS products in CALIBRE Attachment 1, Sample Service Level Agreements.pdf. Due to the rapidly evolving nature of AWS Cloud service offerings, CALIBRE will provide the most current and applicable SLAs for purchasing entities.

8.4.2 Customer Service Requirements

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.*

CALIBRE will comply with the customer service requirements by:

- ▶ Assigning each of our Purchase Entity clients a Project Manager who will serve as the lead representative to execute each Participating Addendum. To provide further corporate contact options, CALIBRE will also assign a Program Manager to oversee the overall Master Agreement contract once awarded. CALIBRE's Contract Manager will keep the contract information current for these employees.
- ▶ Leveraging our corporate service desk to provide support within the required timeframes (Monday through Sunday, 7AM to 6PM for all time zones) along with off-hour/weekend support for critical issues.
- ▶ Responding to inquiries within one business day. CALIBRE will report response times monthly to each Purchasing Entity client, or upon request.
- ▶ Providing full life cycle development and deployment services, including design services along with requirements and verification.
- ▶ Assigning engineers to provide Installation Services for applicable categories and products along with the operational and configuration support.

To provide exceptional service support, CALIBRE will also use the AWS support mechanisms for operational support. In addition, Purchasing Entities can procure AWS Support through CALIBRE to obtain direct AWS assistance. AWS Support is a one-on-one, fast-response assistance channel staffed 24x7x365 with experienced technical support engineers.

AWS Support Features: For access to technical support and additional AWS Support resources, AWS offers plans tailored to fit client's needs. A comparison between Basic, Developer, Business, and Enterprise support is available in Table 2 below, as well as on AWS' Compare AWS Support Plans page.

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

Table 2: AWS Support Features - Highly personalized service support staffed 24x7x365 with experienced technical support engineers.

Feature	Basic	Developer	Business	Enterprise
Client Service – 24x7x365	✓	✓	✓	✓
Support Forums	✓	✓	✓	✓

Feature	Basic	Developer	Business	Enterprise
Documentation, Whitepapers, Best Practice Guides	✓	✓	✓	✓
Access to Technical Support	Support for Health Checks	Email (local business hours)	Phone, Chat, Email (24/7)	Phone, Chat, or Email a TAM (24/7)
Primary Case Handling	Technical Client Service Associate	Cloud Support Associate	Cloud Support Engineer	Sr. Cloud Support Engineer
Users Who Can Create Technical Support Cases		1	Unlimited (AWS Identity and Access Management [IAM] supported)	Unlimited (IAM supported)
Response Time		General guidance: < 24 business hours System impaired: < 12 business hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture Support		General Guidance	Contextual Use Case Guidance	Contextual Application Architecture Guidance
Access to Support API			✓	✓
Third-Party Software Support			✓	✓
AWS Trusted Advisor	4 core checks	4 core checks	Full checks	Full checks
Infrastructure Event Management			Contact Us for Pricing	✓
Direct Access to TAM				✓
Architectural Review				✓
Support Concierge				✓
Training				Access to online self-paced labs
Operations Support				Operational reviews, recommendations, and reporting

AWS Support Pricing: AWS Support tiers include an unlimited number of support cases, with no long-term contracts. Also, with the Business and Enterprise-level tiers, as users' AWS charges grow, they earn volume discounts on their AWS Support costs. Please note AWS performs these calculations on a per-account basis. CALIBRE can assist clients with understanding AWS support pricing and is ready to support with our clients with obtaining the most cost effective support plan needed to meet their requirements.

Contacting AWS Support: Clients can contact AWS Support via the Support Center. Developer-level support clients can open a case online with "Web Support" using a web browser. Business- and Enterprise-level clients may also "Click to Call" to have AWS contact them at any convenient phone number. Enterprise-level clients have direct access to their dedicated Technical Account Manager (TAM).

Chat is another way to contact AWS Support. A chat session will begin in a new browser by clicking on the chat support icon in the Support Center. This provides a real-time, one-on-one interaction with our support engineers and allows for the sharing of additional information for faster issue resolution.

8.5 (E) SECURITY OF INFORMATION

8.5.1 Protecting Data

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.

CALIBRE will use the AWS security tools and features in designing, implementing, and operating a secure AWS environment in conjunction with the Purchasing Entity to reflect the solution requirements. CALIBRE will also recommend additional security tools and controls as needed to perform the required functions. CALIBRE will configure the AWS services to leverage a range of such security features, tools and controls to protect the content, including IAM tools, security capabilities, encryption, and network security.

CALIBRE will work with the Purchasing Entity to establish the appropriate controls over the services and grant access to their content and services, including what credentials they require. CALIBRE will work with each Purchasing Entity to configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change client configuration settings and CALIBRE only does so in consultation with the Purchasing Entity.

Because AWS clients retain ownership and control over their content within the AWS environment, CALIBRE and the Purchasing Entity also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model, shown in Figure 3 below. While AWS manages security of the cloud, security in the cloud is the responsibility of the client.

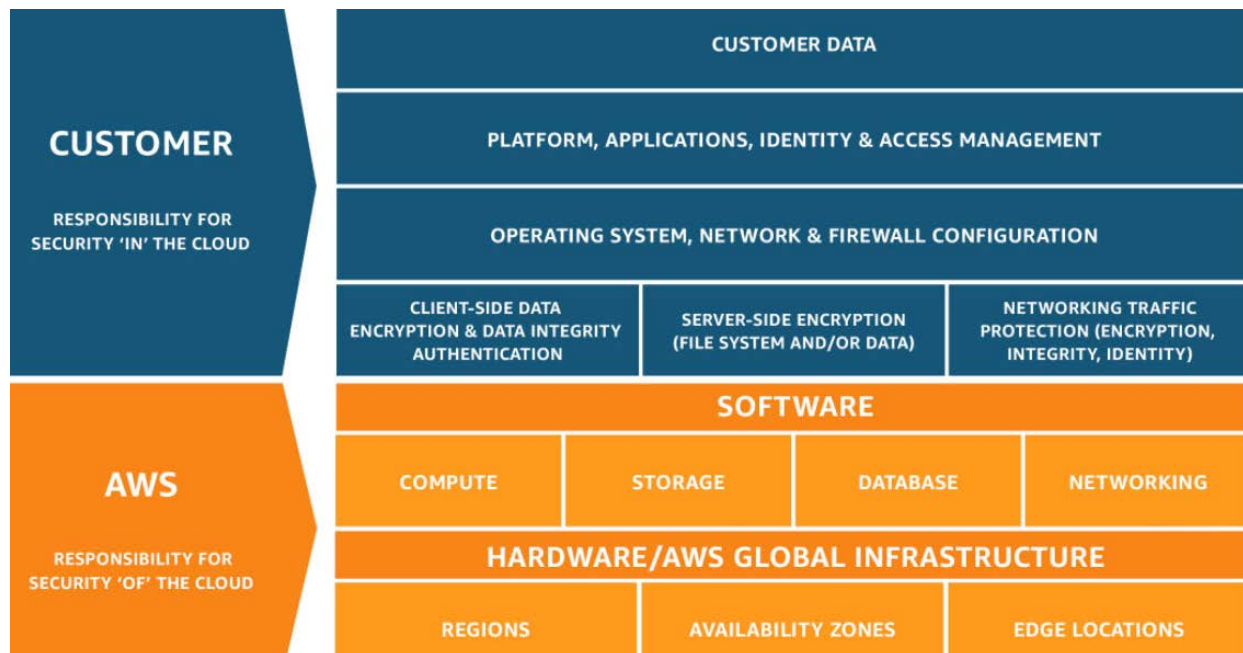


Figure 3: AWS Shared Responsibility Model - Allows clients retain ownership and control over their data and security levels.

Neither CALIBRE nor AWS uses client data or derive information from it for other purposes such as marketing or advertising. AWS does not access or use client data for purposes other than as legally required, and to provide AWS services selected by each client and/or their end users.

AWS data integrity controls as described in AWS SOC reports shows the data integrity controls maintained through all phases including transmission, storage, and processing.

AWS provides clients the flexibility to store data within multiple geographic Regions. Clients designate in which physical region to locate their data and servers. AWS will not move clients' content from the selected Regions without notifying the client, unless required to comply with the law or requests of governmental entities.

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. Decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

8.5.2 Complying with Data Privacy and Security Laws

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

CALIBRE’s ISO and CMMI processes provide the foundation for implementing and securing data in accordance with the applicable privacy and security laws, regulations and requirements.

CALIBRE will leverage the extensive resources AWS applies to its on-going compliance program. AWS has compliance programs for CJIS, CSA, DoD SRG, FedRAMP, FERPA, FIPS, FISMA, ISO 9001, ISO 27001, ISO 27017, ISO 27018, MPAA, NIST, PCI DSS Level 1, SEC Rule 17-a-4(f) and VPAT/508. CALIBRE will work in conjunction with AWS and the

appropriate guidance documents for compliance with legal requirements in applicable areas when establishing and maintaining systems.

8.5.3 Accessing Purchasing Entity's User Accounts and Data

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.

Neither CALIBRE nor AWS uses client data or derive information from it for other purposes such as marketing or advertising. AWS does not access or use client data for purposes other than as legally required, and to provide AWS services selected by each client and/or their end users.

To assist clients in designing, implementing, and operating their own secure AWS environment, AWS provides a wide selection of security tools and features that CALIBRE will use on behalf of the Purchasing Entity. CALIBRE will recommend and implement additional security tools and controls as necessary to meet the security requirements. CALIBRE will configure the AWS services to leverage a range of such security features, tools, and controls to protect their content, including sophisticated IAM tools, security capabilities, encryption, and network security.

8.6 (E) PRIVACY AND SECURITY

8.6.1 Compliance Programs

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.

As described in Section 8.1, CALIBRE will with all aspects of the NIST 800-145 standard and other relevant standards through our relationship with AWS. As part of our pre-engagement with potential Purchasing Entities, CALIBRE will undertake an evaluation of the proposed applications and data risk levels (low, moderate, or high) to establish the appropriate controls, security requirements, and other protective measures. CALIBRE will then validate the assessment during the kickoff meeting and at appropriate times during the engagement period of performance.

8.6.2 Security Certifications

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.

AWS Compliance enables clients to understand the robust controls in place at AWS that facilitate security and data protection in the cloud. AWS designed their cloud infrastructure and manages its alignment with regulations, standards, and best practices, to include:

- ▶ Federal Risk and Authorization Management Program (FedRAMP)
- ▶ System and Organization Controls (SOC) 1, SOC 2, and SOC 3
- ▶ Payment Card Industry Data Security Standard (PCI DSS)
- ▶ International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001

- ▶ Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- ▶ Federal Information Security Management Act (FISMA)
- ▶ US Health Insurance Portability and Accountability Act (HIPAA)
- ▶ FBI Criminal Justice Information Services (CJIS)
- ▶ National Institute of Standards and Technology (NIST) 800-171 and 800-53
- ▶ International Traffic in Arms Regulations (ITAR)
- ▶ Federal Information Processing Standard (FIPS) 140-2
- ▶ Family Educational Rights and Privacy Act (FERPA)
- ▶ Internal Revenue Service Publication 1075 (IRS Pub 1075)

CALIBRE will be the primary driver for FIPS 200. We categorize the information and information system according to the guidelines in the FIPS-199 to establish the appropriate levels of information security according to a range of risk levels (low-impact, moderate-impact or high-impact) for the security objectives of confidentiality, integrity, and availability. The FIPS-199 provides guidelines recommending the types of information and information systems per category and recommended baseline risk level for that category.

Next we apply the minimum information security requirements for that baseline. FIPS Publication 200, the second of the mandatory security standards, specifies minimum security requirements for information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. The minimum security requirements cover 17 security-related areas that protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems.

Organizations must meet the minimum security requirements in the FIPS-200 standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53 (as amended), Recommended Security Controls for Federal Information Systems. Each organization's own policies and procedures govern the minimum security requirements for effective protection of the confidentiality, integrity, and availability for the organization's information and information systems. Organizations must employ all security controls in the respective security control baselines, unless they allow exceptions based on the tailoring guidance provided in NIST Special Publication 800-53. Organizations may apply security control overlays (tailoring recommended controls specific to each agency) on top of the FIPS recommended minimum security requirements to reflect the risk appetite of the organization. This set of activities are beyond the scope of AWS and are within the realm of the CALIBRE support activities for the Purchasing Entities.

8.6.3 Data Security

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.

CALIBRE takes the lead on addressing data security as it is a responsibility of both AWS and their clients. AWS is responsible for the security of the cloud while the client is responsible for the security in the cloud.

AWS manages the security of the underlying cloud environment. AWS designed their cloud infrastructure to be one of the most flexible and secure cloud computing environments available. AWS designed it to provide optimum availability while providing complete client segregation. AWS cloud infrastructure provides extremely scalable, highly reliable services that enable clients to deploy applications and content quickly and securely on a global scale, if necessary.

Security in the cloud is the responsibility of the client. Clients retain ownership and control of their content when using AWS services. Clients, rather than CALIBRE or AWS, determine what content they store or process using AWS services. Because the client decides what content to store or to process using AWS services, only the client can determine what level of security is appropriate for them. Clients also have complete control over which services they use and who they grant access to their content and services, including what credentials they require. Clients control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS and/or CALIBRE do not change client configuration settings, as these settings are client determined and controlled. AWS clients have complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers clients to decide when and how to implement security measures in the cloud. For example, if a client requires a higher availability architecture to protect content, the client may add redundant systems, backups, locations, and network uplinks to create a more resilient, high availability architecture. If clients need to restrict access to content, AWS enables them to implement access rights management controls both on a systems level and through encryption on a data level.

AWS has many responsibilities in providing security of the cloud. To do this, AWS uses monitoring tools they 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.

AWS instrumented systems extensively to monitor key operational metrics. Alarms automatically notify operations and management personnel when early warning thresholds on key operational metrics are crossed. AWS uses an on-call schedule so personnel are available to respond to operational issues. This includes a pager system to communicate alarms quickly and reliably to operations personnel.

AWS maintains documentation to aid and inform operations personnel when handling incidents or issues. If the resolution of an issue requires collaboration, a trained call leader will use a conferencing system to facilitate communication and progress during the handling of operational issues. Call leaders coordinate post-mortems after any significant operational issue, regardless of external impact. Call leaders draft Cause of Error documents to capture the root cause and preventative actions required in the future. Call leaders track the implementation of the preventative measures during weekly operations meetings.

AWS security monitoring tools identify several types of Denial of Service (DoS) attacks, including distributed, flooding, and software/logic attacks. Monitoring tools start the AWS incident response when they identify a DoS attack. In addition to DoS prevention tools,

redundant telecommunication providers at each region, as well as additional compute capacity, protect against the possibility of DoS attacks.

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

- ▶ **Distributed Denial of Service (DDoS) Attacks** - AWS hosts API endpoints on large, Internet-scale, world-class infrastructure. AWS leverages Proprietary DDoS mitigation techniques. Additionally, AWS's networks are multi-homed across several providers to achieve Internet access diversity.
- ▶ **Man in the Middle (MITM) Attacks** - All of the AWS APIs are available via Secure Sockets Layer (SSL)-protected endpoints that provide server authentication. Amazon EC2's Amazon Machine Images (AMIs) automatically generate new Secure Shell (SSH) host certificates on first boot and log them to the instance's console. Users 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 clients to use SSL for 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 clients are a violation of the AWS Acceptable Use Policy. AWS takes violations of their Acceptable Use Policy seriously, and they investigate every reported violation. Clients can report suspected abuse via the contacts available on AWS' website at: <http://aws.amazon.com/contact-us/report-abuse/>. AWS stops and blocks an unauthorized port scan when AWS detects them. Port scans of Amazon EC2 instances are generally ineffective because, by default, inbound ports on Amazon EC2 instances are closed. Only the user can open them. Clients' strict management of security groups can further mitigate the threat of port scans. If users configure the security group to allow traffic from any source to a port, then that port will be vulnerable to a port scan. In these cases, users must use appropriate security measures to protect application essential listening services from an unauthorized port scans' detection. 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. Users may request permission to conduct vulnerability scans as required to meet their compliance requirements. The user must limit scans to their own instances and must not violate the AWS Acceptable Use Policy. CALIBRE can provide support in obtaining advanced approval for these types of scans.
- ▶ **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 users can place their interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even if a client owns two virtual instances that are located on the same physical host, they cannot listen to each other's traffic. Attacks such as Address Resolution Protocol (ARP) cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one client inadvertently or maliciously attempting to view another's data, as a standard practice, users should encrypt sensitive traffic.

In addition to protecting this global infrastructure, AWS is responsible for the security configuration of its managed services products. Examples of these types of services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces, and several other services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit AWS' management of them. For these services, AWS will handle basic security tasks like guest Operating System and database patching, firewall configuration, and disaster recovery.

8.6.4 Data Confidentiality Standards

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

CALIBRE develops, documents, and disseminates to employees a data systems and communications protection policy. It addresses purpose, scope, roles, responsibilities, management commitment, coordination among stakeholders, and compliance and procedures. The policy also aids to facilitate the implement its associated system controls. During the life cycle of the NASPO Master Agreement, CALIBRE will regularly review and update the policy and procedures, or when significant system changes occur.

CALIBRE maintains a wide variety of protective measures on our corporate hardware. We manage access to our computers through two-factor authentication using RSA and each laptop has an encrypted hard drive. CALIBRE secures access to our VPN using GlobalProtect. We manage access to mobile phones that access corporate resources or email through ActiveSync. ActiveSync implements required protective measures and the ability for remote data wipes in the event of loss.

CALIBRE will support our clients as needed with using and assigning the appropriate groups and roles permissions defined in AWS Identity & Access Management (IAM). This will prevent the presentation of information system management-related functionality for non-privileged users. AWS VPC separates security controls from Operational controls as the client is required to assign strict permissions to IAM accounts or roles. For example, a user identity for a staff member who manages EC2 instances will not be able to view or modify IAM settings.

The security strategy deployed by CALIBRE in AWS is Deny by Default that configures Communications and permissions between resources in an Amazon VPC. We follow AWS best practices, with an allow rule added as a documented exception.

Volumes, either attached to EC2 instances or unattached as snapshots, are encrypted using certificates managed by AWS Key Management Services. AWS can either generate or import certificates that Key Management Service (KMS) manages.

S3 Buckets default configuration is to allow unsecure HTTP connection. The needs of most projects require S3 buckets to only accept secure HTTPS connections. CALIBRE writes the JavaScript Object Notation (JSON) document required to harden S3 buckets in this way.

AWS does not access client data. AWS gives clients the choice regarding how they store, manage, and protect their data.

8.6.5 Third-Party Attestations

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.

The AWS Cloud infrastructure has third-party attestations, reports, credentials, and certifications for the following:

- ▶ Federal Risk and Authorization Management Program (FedRAMP)
- ▶ System and Organization Controls (SOC) 1, SOC 2, and SOC 3
- ▶ Payment Card Industry Data Security Standard (PCI DSS)
- ▶ International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001
- ▶ Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- ▶ Federal Information Processing Standard (FIPS) 140-2
- ▶ SEC Rule 17-a-4(f)

AWS also provides best practices and guidance to assist in compliance with other laws, regulations and standards where there is no certifying body (such as CJIS, FERPA, FISMA, HIPAA, ITAR, and NIST).

8.6.6 Logging Process

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

The AWS logging and monitoring of API calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS clients can leverage multiple AWS features and capabilities, along with third-party tools, to monitor their instances and manage / analyze log files. AWS provides AWS CloudTrail, CloudWatch, VPC Flow Logs, and LogAnalyzer for Amazon CloudFront as logging and monitoring options in AWS, as described below.

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 clients to enhance security and operational processes while demonstrating compliance with policies or regulatory standards.

With AWS CloudTrail, clients 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. CloudTrail allows clients to deep dive into all AWS API calls with information such as device SourceIP, event name, event time, event source and username. CALIBRE is also able to integrate CloudTrail logs easily with third-party log management solutions such as AlertLogic, Boundary, Loggly, Splunk, and Sumologic.

AWS CloudTrail's Features and Benefits: Some of the features of AWS CloudTrail include:

- ▶ **Increased Visibility** - AWS CloudTrail provides increased visibility into user activity by recording AWS API calls. Clients 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? What activities failed due to inadequate permissions?
- ▶ **Durable and Inexpensive Log File Storage** - AWS CloudTrail uses Amazon S3 for log file storage and delivery to durably and inexpensively store log. Clients can use Amazon S3 lifecycle configuration rules to further reduce storage costs. For example, clients 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. Clients 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** - Clients can configure AWS CloudTrail to publish a notification for each log file delivered, thus enabling clients 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.
- ▶ **Log File Aggregation** - Clients can configure AWS CloudTrail to aggregate log files across multiple accounts and regions to deliver log files to a single bucket.

AWS CloudWatch: AWS CloudWatch is a monitoring service for AWS Cloud resources and the applications run on AWS. Clients 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 client applications and services, and any log files that applications generate. Clients 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. Clients can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Clients can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time.

VPC Flow Logs: VPC Flow Logs is a feature that enables clients to capture information about the IP traffic going to and from network interfaces in Amazon VPC. Amazon CloudWatch Logs stores the flow log data. Flow logs assist with several tasks; for example, to troubleshoot why traffic is not reaching an instance, which enable diagnoses of overly restrictive security group rules. Clients use flow logs as a security tool to monitor the traffic that is reaching the instance.

LogAnalyzer for Amazon CloudFront: LogAnalyzer for CloudFront allows clients to analyze their CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application clients can generate usage reports containing total traffic volume, object popularity, a breakdown of traffic by client IPs, and edge location. Amazon

EMR and the LogAnalyzer format these reports as tab delimited text files, and deliver them to the Amazon S3 bucket that clients 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.

LogAnalyzer Generated Reports: This LogAnalyzer application produces four sets of client customizable reports based on Amazon CloudFront access logs to include:

- ▶ The Overall Volume Report displays total amount of traffic delivered by CloudFront over the course a specified period.
- ▶ The Object Popularity Report shows how many times the client requested each object.
- ▶ 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, total number of bytes transferred, and number of request broken down by HTTP response code. Cascading (<http://www.cascading.org>) implements the LogAnalyzer and is an example of how to construct an Amazon Elastic MapReduce application.

AWS engages with external certifying bodies and independent auditors to provide clients with considerable information regarding the policies, processes, and AWS established and operated controls. AWS' Compliance and Security teams established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. AWS 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 NIST Publication 800-53 Revision 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 and conformance to the information security policy. These efforts support AWS in maintaining their security certifications including for DoD SRG, FedRAMP, FIPS, ISO 9001, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SEC Rule 17-a-4(f).

8.6.7 Restrict Visibility of Cloud Hosted Data

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

CALIBRE will work with the Purchasing Entities to establish the appropriate access controls and visibility into cloud hosted data and documents. CALIBRE will use the AWS IAM that enables clients to securely control their user access to AWS services and resources. Using IAM, clients create and manage AWS users and groups. Clients use permissions to allow and deny access to AWS resources. IAM allows users to:

- ▶ **Manage IAM users and their access** – Clients can create users in IAM, assign them individual security credentials, such as access keys, passwords, and multi-factor

authentication devices, or request temporary security credentials to provide users access to AWS services and resources.

- ▶ **Manage IAM roles and their permissions** – Users can create roles in IAM, and manage permissions to control what operations a user can perform, for each role. Users also define which entity to allow to assume a role.
- ▶ **Manage federated users and their permissions** – Clients can enable identity federation to allow existing identities, such as users, in their enterprise to access the AWS Management Console, to call AWS APIs, and to access resources, without the need to create an IAM user for each identity.

8.6.8 Notification Process for Security Incident

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.*

CALIBRE will leverage AWS' various methods of communication to support its client base and the community. CALIBRE receives notification and alerts from AWS either through the public Rich Site Summary (RSS) feeds, Service Health Dashboard or directly from client services concerning security incidents. CALIBRE will parse the notification for relay. In order to accommodate the different notification requirements and timelines for individual Purchasing Entity's laws and requirements for types of data, CALIBRE will develop a detailed notification plan for each Purchasing Entity. The notification plan will address the points of contacts, timing based on incident level, criticality and data sensitivity. The plan will outline the expected SLAs and milestones to address at each stage of the incident.

8.6.9 Isolation of Host Servers

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.*

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 client from other clients in their implementation of Zones of Control Architectures (ZOCA). AWS designed their systems to prevent clients from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. An independent PCI Qualified Security Assessor validated this architecture and found that it complied with all requirements of PCI DSS Security Standards 3.2 as of July 2016.

AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within users' Amazon VPC that run hardware dedicated to a single client. Dedicated Instances let users utilize the benefits of Amazon VPC and AWS Cloud while isolating their Amazon EC2 compute instances at the hardware level. Figure 4 below shows AWS isolation and deployment options.

Because AWS clients retain ownership and control over their content within the AWS environment for all service models (IaaS, PaaS, and SaaS), they also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model, shown

in Figure 3 in section 8.5.1 Protecting Data. The “shared responsibility” model displays the zones in which AWS and the client have responsibilities to manage.

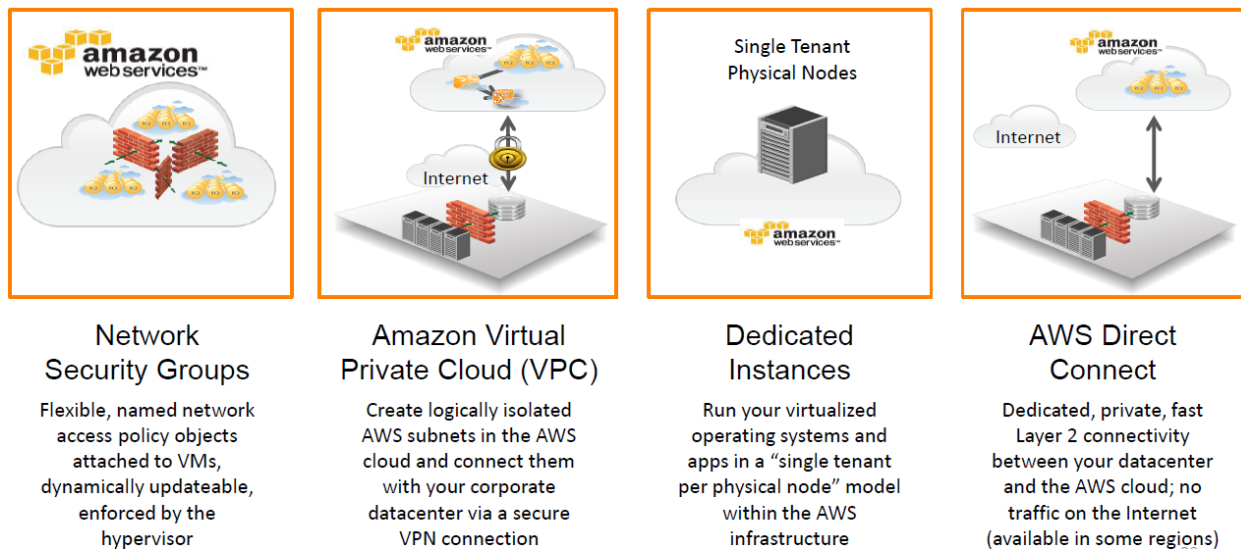


Figure 4: AWS Isolation and Deployment - AWS designed their systems to prevent clients from accessing physical hosts or instances not assigned to them.

8.6.10 Security Technical Reference Architectures

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 5 shows the AWS Enterprise Security Reference Architecture for IaaS, PaaS, and SaaS components. The AWS overarching technical security reference model is then extended to provide the appropriate protections for each implementation.

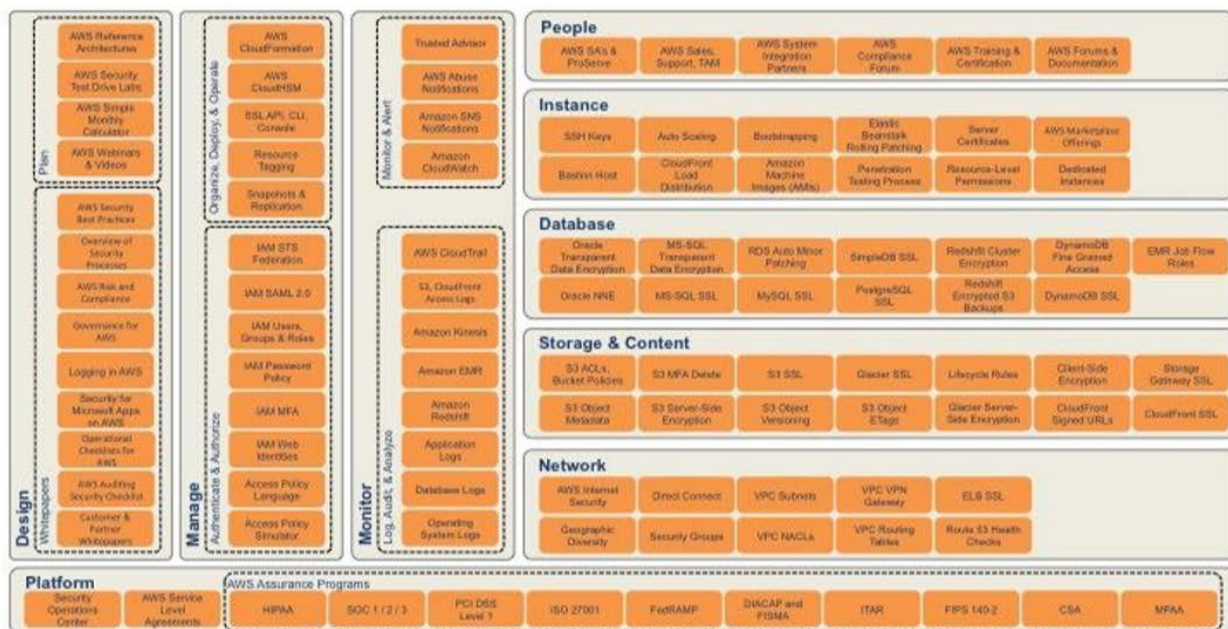


Figure 5: AWS Enterprise Security Architecture - AWS protects their system components under a wide variety of standards and across the IaaS, PaaS and SaaS environments.

8.6.11 Security Procedures for Employees

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.

CALIBRE has established staffing policies and procedures that require that employment is conditional upon the results of reference checks and security investigations. We require each employee to take annual security training that reinforces and explains the necessary sets for protecting computer resources and sensitive data. As needed, CALIBRE also provides training for individual projects and clients such as HIPAA and DoD Cleared Staff. Misrepresentation or omission of facts called for on application forms or other documents is cause for dismissal.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and clients are responsible for securing the workloads they deploy in AWS. AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The AWS SOC reports provide additional details regarding the controls in place for background verification.

8.6.12 Security of Confidential Data at Rest and In Transit

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.

AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls, as well as additional FedRAMP requirements. AWS has received FedRAMP ATO from multiple authorizing agencies for the AWS GovCloud (US) Region and the AWS US East/West Region.

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

- ▶ Data encryption capabilities in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Oracle RDS, SQL Server RDS, and Amazon Redshift.
- ▶ Flexible key management options, including AWS' KMS that allow clients to choose whether to have AWS manage the encryption keys or keep complete control over their keys.
- ▶ Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing clients to satisfy compliance requirements.
- ▶ Support for Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit.
- ▶ APIs for clients to integrate encryption and data protection with any of the services developed or deployed in an AWS environment.
- ▶ In addition to the AWS services, clients can use file system encryption. File-system-level encryption operates on top of the file system and is portable across operating systems.

8.6.13 Notification of Cardholders Data Breach

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.

CALIBRE is responsible for monitoring the Purchasing Entities' systems and responding in accordance with our data breach process in Section 8.3.1 Data Breach. CALIBRE will notify the State via email and phone call. CALIBRE will then establish the processes and mechanisms for cardholder notifications with the State (such as email or mailing a letter). AWS has performed mitigation through the PCI DSS and CALIBRE will implement the recommended AWS best practices and relevant guidance for any system with card data.

8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

8.7.1 End of Life Activities

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.

CALIBRE will work closely with Purchasing Entities in advance of end of life activities to provide an orderly and secure transition of data. CALIBRE will prepare a Transition Plan that lays out the required activities with shutting down a service. The plan will layout the coordination with Purchasing Entity on the following activities:

- ▶ Removal of user accounts and/or access rights
- ▶ User communications
- ▶ On-going operational requirements during disposition process
- ▶ Archival and Export of Data
- ▶ Transfer mechanism to Purchasing Entity
- ▶ Turn-Down of applications and systems
- ▶ Disposal of software
- ▶ Elimination of obsolete security authentication and authorizations
- ▶ Final reports and security validations

8.7.2 Return of Data

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 client.

CALIBRE administers solutions on behalf of the Purchasing Entities who retain control and access rights in accordance with their account agreement. In cooperation with, and at the direction of, the Purchasing Entity, we will establish the process for the orderly return of data. In practice, Purchasing Entities can transfer data to their on-premise sites at any time through their authorized administrators using a number of options such as direct file transfers across the network or FTP/SFTP sites. Data transfer options and SLAs will vary according to data size, sensitivity, network configurations, and ability to use external devices. CALIBRE will establish

the SLAs for data transfer upon a service ending as part of the underlying agreement with the Purchasing Entity.

8.8 (E) SERVICE OR DATA RECOVERY

8.8.1 Contingency Plan

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:** CALIBRE will configure AWS to back up the data on Amazon EBS volumes to Amazon S3 by taking point in time AMI, or snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after the most recent snapshot. When extended downtime occurs, CALIBRE will launch snapshots of down instances in another Availability Zone
- b. **Suffers an unrecoverable loss of data:** CALIBRE recommends regular snapshots of Relational Database Service (RDS) instances to prevent the unrecoverable loss of database data. AWS does not delete manual snapshots with the RDS instance and CALIBRE can recover the database from a manual snapshot. AWS storage is designed to operate without a loss of data through a number of techniques. However, CALIBRE will implement a regular back-up schedule, in consultation with the Purchasing Entity, to address unforeseen circumstances.
- c. **Offeror experiences a system failure:** CALIBRE designs recoverability into our solutions in consultation with the Purchasing Entity. The design will accommodate the various levels of systems failures throughout the technology stack starting with AWS infrastructure and going up through networks, operating system, and application layer. There is a direct correlation between the ability to recover from a system failure and the costs to implement and run these efforts. For example, a mission critical financial system has a higher level of effort than a timesheet system. CALIBRE will optimize costs and requirements to provide the best value considering the solution needs.
- d. **Recover and restore data:** Snapshots and backup data stored in S3 are available over multiple availability zones in AWS. In the event of a severe system failure, snapshot data and backups stored in S3 can brought online in another availability zone. CALIBRE can perform the necessary restoration processes in four hours from the determination that the recovery is required and based on the overall availability of AWS services.
- e. **Recovery Point Objective (RPO) and Recovery Time Objective (RTO):** CALIBRE will establish the RPO and RTO with the Purchasing Entity to match the system criticality and cost considerations. Due to the flexibility of AWS, CALIBRE can design the solution based on the desired RTO and RPO. If the RTO and RPO is set to be more than 73 hours, then daily snapshots are taken. S3 stores the snapshots to span a minimum

of three availability zones (Availability zones are separate locations within the same region joined by low-latency links.) When necessary, CALIBRE can enact recovery within the VPC using any of the availability zones that data resides in. If CALIBRE has set the RTO to 4 hours and the RPO to 1 hour, then S3 takes snapshots every 30 minutes.

8.8.2 Backup and Restore Services

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.**

CALIBRE develops a robust back-up strategy for each Purchasing Entity that addresses their specific needs and implementation. CALIBRE will back up the data on Amazon EBS volumes to Amazon S3 by taking point in time AMIs (snapshots). Snapshots are incremental backups, which means that AWS only saves the updated / changed blocks on the device since the previous snapshot. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. Each snapshot contains the information needed to restore the data (from the moment when the snapshot occurred) to a new EBS volume.

AMI provides the information required to launch an instance. An AMI includes the following:

- ▶ A template for the root volume for the instance, such as an operating system, application server, and applications.
- ▶ Launch permissions that control what AWS accounts can use the AMI to launch instances.
- ▶ A block device mapping that specifies the volumes to attach to the instance when launched.

AWS snapshots and AMI are constrained to the region where it was created. However, CALIBRE can copy the AMI within or across an AWS region using the AWS Management Console, the AWS Command Line Interface (CLI), or SDKs, or the Amazon EC2 API, all of which support the CopyImage action. CALIBRE can also copy AWS snapshots from one region to another depending on the requirements for the solution and disaster recovery parameters. Amazon S3 server-side encryption (256-bit Advanced Encryption Standard (AES)) protects a snapshot's data in transit during a copy operation.

AWS Regions and Availability Zones: AWS built their Cloud infrastructure around Regions and Availability Zones (AZs), as shown in Figure 6. AWS regions provide multiple, physically separated and isolated AZs. They are connected with low-latency, high throughput, and highly redundant networking. These AZs offer AWS clients an easier and more effective way to design and operate applications and databases. Thus, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures.

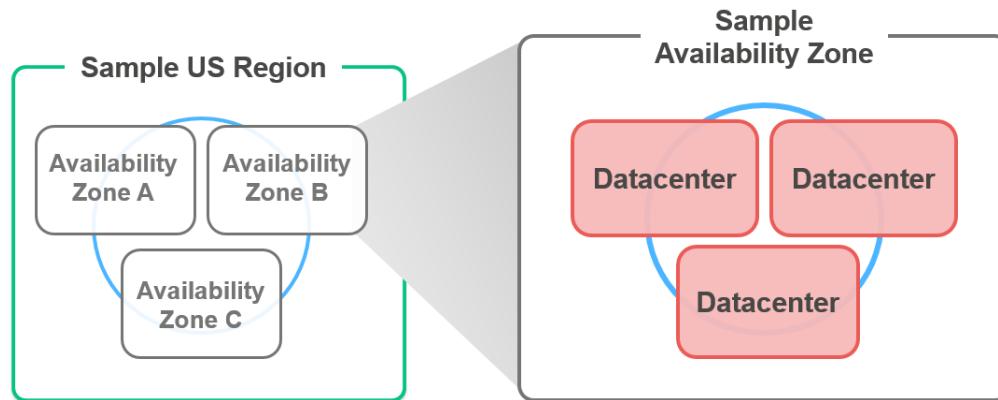


Figure 6: Regions and Availability Zones - Provides users with the flexibility to place instances and store data within multiple geographic regions as well as across multiple AZs within each region.

AWS replicates critical system components across multiple AZs to provide high availability under normal circumstances and during disasters such as fires, tornadoes, or floods. AZs consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS AZ runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single AZ. AWS designs their data centers' electrical power systems to be fully redundant and maintainable without impact to operations. AWS data centers do not share common points of failure, such as generators, Uninterruptable Power Supply (UPS) units, and air conditioning across AZs.

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

Availability and Fault Tolerant Design: Amazon's infrastructure has a high-level of availability and provides users with the capability to deploy a resilient IT architecture. AWS designed its systems to tolerate system or hardware failures with minimal client impact.

AWS built data centers in clusters in various global regions. All data centers are online and serving clients; no data center is "cold." In case of failure, automated processes move client data traffic away from the affected area. AWS deploys core applications 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 users with the flexibility to place instances and store data within multiple geographic regions as well as across multiple AZs within each region. AWS designed each as an independent failure zone and physically separated them within typical metropolitan regions and in lower risk flood plains (flood zone categorization varies by Region). In addition to discrete UPS and on-site backup generation facilities, different grids from independent utilities feed each data center to further reduce single points of failure. AWS redundantly connected AZs to multiple tier-1 transit providers.

Users should architect their AWS usage to take advantage of multiple regions and AZs. Distributing applications across multiple AZs provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures. However, users should be

aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Only the client can proactively replicate data between regions, thus allowing clients with these types of data placement and privacy requirements the ability to establish compliant environments. Note that communications between regions is across the public Internet infrastructure. Therefore, the client should use the appropriate encryption methods to protect sensitive data.

AWS currently has 18 regions, 54 AZs, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local Region), South America (Sao Paulo), China (Beijing), and China (Ningxia). The AWS Global Infrastructure webpage contains more information on each region. Figure 7 depicts the current AWS regions and AZs, along with the four new regions that AWS has announced plans to expand.



Figure 7: Global Map of AWS Regions and Availability Zones - Offer clients the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.

AWS designed the AWS GovCloud (US) as an isolated AWS region to allow US Government agencies to move and operate workloads in the cloud; thus enabling them meet certain regulatory and compliance requirements. The AWS GovCloud (US) framework allows US Government agencies and their contractors to comply with U.S. ITAR regulations as well as the FedRAMP requirements. AWS GovCloud (US) has received an ATO from the US Department of Health and Human Services (HHS) using a FedRAMP accredited Third-Party Assessment Organization (3PAO) for several AWS services.

The AWS GovCloud (US) Region provides the same fault tolerant design as other regions, with two AZs. In addition, the AWS GovCloud (US) region is a mandatory Amazon VPC service by default to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses. More information about GovCloud is available on the AWS website: <http://aws.amazon.com/govcloud-us/>.

8.9 (E) DATA PROTECTION

8.9.1 Standard Encryption Technologies

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.*

Because AWS clients retain ownership and control over their content within the AWS environment for all service models (IaaS, PaaS and SaaS), they also retain responsibilities relating to the security of that content as part of the AWS “shared responsibility” model, shown in Figure 3 in section 8.5.1 Protecting Data. Below we describe AWS encryption technologies and options to protect sensitive data.

Securing Data at Rest: Encrypting data at rest is vital for regulatory compliance so that sensitive data saved on disks is not readable by any user or application without a valid key. Compliance regulations, such as PCI DSS and HIPAA, require that data at rest be encrypted throughout the data lifecycle. AWS provides several options for encrypting data at rest, ranging from completely automated AWS encryption solutions, such as AWS KMS, to manual, client-side options like AWS CloudHSM. Choosing the right solution depends on which AWS Cloud services the client uses and the client’s requirements for key management. For example, clients can encrypt Amazon EBS volumes and configure Amazon S3 buckets for server-side encryption (SSE) using AES-256 encryption. Additionally, Amazon RDS supports Transparent Data Encryption (TDE).

Securing Data in Transit: AWS shared responsibility model dictates governance of protecting data in transit, which provides capabilities for the application owner. Security of data in transit is the responsibility of the application owner to apply the correct security measures for their environment. CALIBRE is available to provide guidance to application owners in applying proper security in the cloud. The application owner is responsible for using proper technology to secure data in transit that is not between AWS services.

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers, and network traffic between servers. Traffic between AWS services is encrypted with TLS. In addition services from AWS provide support for Internet Protocol Security (IPSec) and 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.

8.9.2 Business Associate Agreement

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.*

AWS has a standard Business Associate Addendum (BAA) that CALIBRE will present to clients for signature. It takes into account the services AWS provides and accommodates the AWS Shared Responsibility Model. CALIBRE is willing to sign relevant and applicable BAA or any other agreement that may be necessary to protect data with a purchasing entity, provided that said agreement does not conflict or breach any aspects of existing agreements or exceeds the capabilities of our service providers. Additionally, CALIBRE will present the AWS Public

Sector Access Policy which provides the rules, conditions, and restrictions regarding the use of AWS cloud services through a reseller such as CALIBRE. CALIBRE provided this information in the document titled CALIBRE Attachment 2, AWS Public Sector Access Policy.

8.9.3 Use of Government Data

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.

Neither CALIBRE nor AWS uses client data or derive information from it for other purposes such as marketing or advertising. AWS does not access or use client data for purposes other than as legally required, and to provide AWS services selected by each client and/or their end users. CALIBRE will only use data for the purposes defined in the Master Agreement, participating addendum, and related SLA. CALIBRE will not data mine client's data unless expressly required by the client and will not sell nor distribute client data for any purpose. CALIBRE and AWS have policies and procedures that employees must follow when dealing with client data.

8.10 SERVICE LEVEL AGREEMENTS

8.10.1 Negotiating the Service Level Agreement

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 has millions of active clients and AWS offers the same portfolio of self-service, highly automated web services to its clients on a one-to-many basis. Because of this, AWS cannot commit to keep the services or SLAs the same for certain clients, but improve or change them for others. AWS requires the right to make changes across its client base, and is not able to offer users a custom notice period. The SLAs offered for cloud services are generally not negotiable based on the requirements of the purchasing entity. As CALIBRE does not hold SLAs for the cloud services, we will work with purchasing entities to modify and negotiate changes where allowable by our partner AWS.

8.10.2 Sample Service Level Agreement

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.

CALIBRE has included the following sample SLAs which define performance and other operating parameters. As our provider, AWS provides SLAs that apply to client use of services. Due to the rapidly evolving nature of AWS Cloud service offerings, CALIBRE will provide the most current and applicable SLAs for purchasing entities. CALIBRE provides the following sample SLAs in Attachment 1, Sample Service Level Agreements:

- ▶ Amazon Compute SLA
- ▶ Amazon Simple Storage Service (Amazon S3) SLA
- ▶ Amazon CloudFront SLA
- ▶ Amazon Route 53 SLA

- ▶ Amazon Relational Database Service (Amazon RDS) SLA
- ▶ AWS Shield Advanced SLA

8.11 (E) DATA DISPOSAL

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

AWS clients retain control and ownership of their data, and it is the client's responsibility to manage their data. Therefore, clients have the ability to delete their data.

AWS Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process to prevent unauthorized individuals access to client data. 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. Decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

8.12 (E) PERFORMANCE MEASURES AND REPORTING

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

AWS takes extensive precautions to remain fully operational, with no loss of service for hosted applications. AWS does not have a Certified Uptime Tiering level; however, AWS operates data center environments using N+1 architecture. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95%, and Amazon S3 with an SLA of 99.9%. AWS details its generator backup capabilities in their SOC Reports, as is the AWS information regarding business continuity planning and N+1 architecture.

AWS replicates critical system components across multiple AZs to provide high availability under normal circumstances and during disasters such as fires, tornadoes, or floods. AZs consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS AZs runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single AZs. AWS designed their data centers' electrical power systems to be fully redundant and maintainable without impact to operations. AWS data centers do not share common points of failure, such as generators, UPS units, and air conditioning across AZs.

AWS plans for failure by maintaining contingency plans and regularly rehearsing our responses. In the words of Werner Vogels, Amazon's CTO: "Everything fails, all the time." We regularly perform preventative maintenance on our generators and UPS units so that equipment is ready when needed. AWS also maintain a series of incident response plans covering common and uncommon events, and update them regularly to incorporate lessons learned and prepare for emerging threats.

While AWS goes to great lengths to provide availability of the cloud, clients share responsibility for availability within the cloud. These clients and others like them have succeeded because they designed for failure and have adopted best practices for high availability, such as taking advantage of multiple AZs and configuring Auto Scaling groups to replace unhealthy instances. In addition, the AWS "Well-Architected Framework" codifies the experiences of thousands of

clients, enables clients to assess and improve their cloud-based architectures and mitigate disruptions.

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

8.12.2 Standard Uptime Service

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

Our standard uptime service and SLA criteria is address through those provided by AWS. The uptime SLAs vary by product and AWS addresses them in related SLA documents. CALIBRE will provide the Purchasing Entities with the expected uptime and SLAs for the services implemented for their solution. As an example, AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95%, and Amazon S3 with an SLA of 99.9%. CALIBRE has provided samples of AWS SLA's offered in Attachment 1, Sample Service Level Agreements.

8.12.3 Support Process

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.

CALIBRE will use our ISO 20000 certified service desk to support the participating entity. We will provide the Participating Entity the phone number, email address, and website for opening support requests at the kickoff meeting. Our service desk will then provide tier 1 support to address the issue and initial resolution efforts. CALIBRE will escalate unresolved issues to our tier 2 and 3 AWS support engineers. As necessary, our CALIBRE staff will open tickets with the AWS support team and manage the ticket to completion. CALIBRE will staff the service desk during the defined business hours will support available off-hours and weekends for critical issues. In the event of significant issues, CALIBRE support staff will notify the Purchasing Entity along with our Contract Manager and Deputy Contract Manager to provide direct response visibility. Our contracts staff is available during normal business hours with additional availability for emergency situations.

8.12.4 SLA Remedies – Incident Response Time

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

CALIBRE provides IaaS, PaaS, and SaaS offering that uses AWS as its Cloud Service Provider. Since SLA remedies and associated details vary with contracted products and services, CALIBRE has provided samples of the applicable AWS SLA's offered in Attachment 1, Sample Service Level Agreements. They provide applicable consequences / SLA remedy review and associated credit policies.

8.12.5 Planned Downtime

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

CALIBRE develops the schedule for planned downtime directly with the Purchasing Entity to accommodate the unique requirements of the application, operational environment and

regulatory requirements. CALIBRE will provide a minimum notice of three working days to the participating entity for planned downtime outside the regularly scheduled windows. We planned downtime will develop a preliminary plan, length of time and schedule for the downtime. CALIBRE will contact the entity to inquire if the preliminary outage schedule will disrupt the participating entity. The participating entity will then contact the appropriate internal units for mutual approval of the schedule. When they mutually agreed upon and approve the schedule for the downtime, the participating entity will contact CALIBRE with the schedule date and length of time of the downtime.

AWS does not need to bring systems offline to perform regular maintenance and system patching. AWS' maintenance and system patching generally do not impact clients. There may be occasions when AWS schedule a client instance for a reboot for maintenance, such as applying updates that require a reboot. AWS does not require action on the client's part, as reboots occur within the client's scheduled window. These scheduled events are not frequent. If a scheduled event will affect a client instance, AWS will communicate with CALIBRE, either via email, or through the AWS Service Health Dashboard before the scheduled event with details and a start and end date. Clients can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI.

8.12.6 SLA Remedies – Disaster Recovery

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

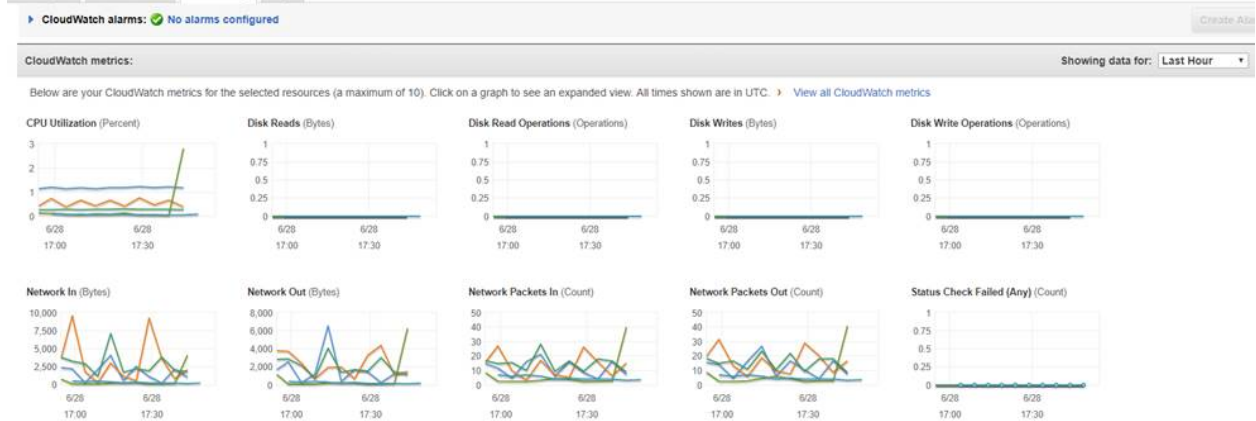
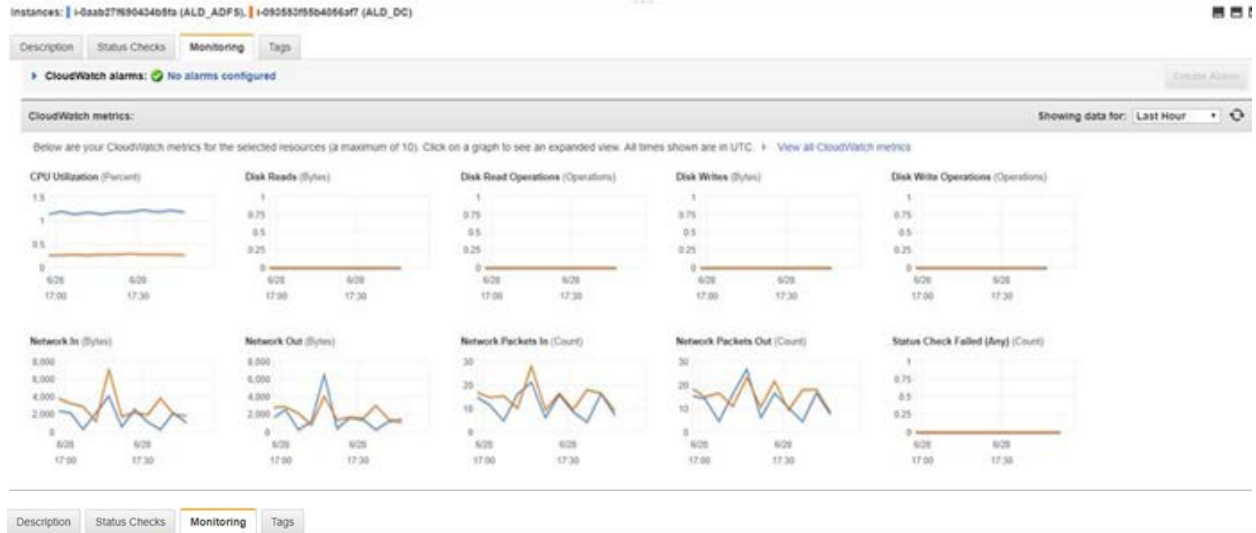
CALIBRE provides IaaS, PaaS, and SaaS offering that uses AWS as its Cloud Service Provider. Since SLA remedies and associated details vary with contracted products and services, CALIBRE has provided samples of the applicable AWS SLA's offered in Attachment 1, Sample Service Level Agreements. They provide applicable consequences / SLA remedy review and associated credit policies.

The AWS Cloud supports many popular disaster recovery architectures, ranging from "pilot light" environments that are ready to scale-up at a moment's notice, to "hot standby" environments that enable rapid failover. All data centers are online and serving clients; no data center is "cold." In the case of a failure, automated processes move client data traffic away from the affected area. By distributing applications across multiple AWS AZs, users can remain resilient in the face of most failure modes, including natural disasters or system failures. Users can build highly resilient systems in the cloud by employing multiple instances in multiple AWS AZs and using data replication to achieve extremely high recovery time and RPOs. Users manage and test the backup and recovery of their information system that they build on the AWS infrastructure. Clients can use the AWS infrastructure to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. CALIBRE provides clients with support should they need or experience a disaster recovery effort.

8.12.7 Sample of Performance Reports

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.

In addition to the capabilities provided by AWS, CALIBRE is able to implement third-party software such as Idera Infrastructure monitor to provide additional performance monitoring and reporting capabilities. Figure 8 shows a set of sample AWS Performance Reports.



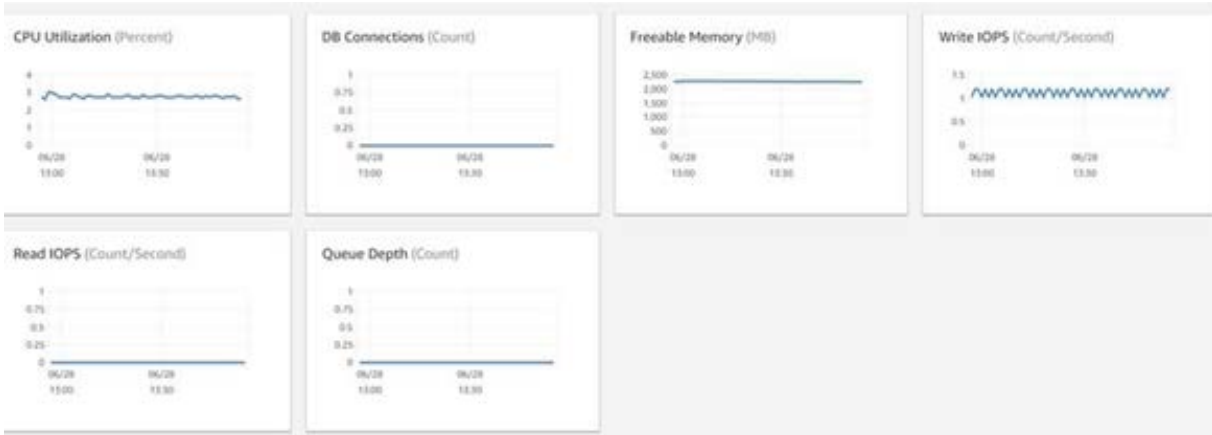


Figure 8: Sample AWS Reports – AWS provides a wide range of reports for the various services and components.

AWS clients can leverage AWS Cloud monitoring tools such as Amazon CloudWatch, AWS Trusted Advisor, AWS Health Checks, and third-party monitoring tools to extract metrics and system analytics. The AWS Service Health Dashboard provides current and historical data across regions for each service offered. Clients can monitor status in real-time, or subscribed to as an RSS feed by service.

8.12.8 Ability to Print Historical, Statistical, and Usage Reports

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

The AWS billing dashboard provides the capability to generate historical cost and usage reports. The AWS Cost and Usage report provides clients information about the use of AWS resources and estimated costs for that usage. Clients can use the AWS billing dashboard to show information such as how many hours of EC2 they used over a time period.

LogAnalyzer Generated Reports: The CloudFront LogAnalyzer application produces four sets of client customizable reports based on Amazon CloudFront access logs to include:

- ▶ Overall Volume Report displays total amount of traffic delivered by CloudFront over the course of a specified period.
- ▶ Object Popularity Report shows how many times the client requested each object.
- ▶ Client IP report shows traffic from each different Client IP that made a request for content.
- ▶ 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.

CALIBRE has the ability to implement third-party tools to supplement AWS built in capabilities for full printing and viewing capabilities of historical, statistical and usage reports that exceed the online reports.

8.12.9 24x365 On-Demand Deployment

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

AWS supports on-demand deployment 24x7x365. CALIBRE will work with Purchasing Entities to enable direct deployments as needed.

8.12.10 Scale-up and Scale-down

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

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

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

Auto Scaling enables clients to closely follow the demand curve for their applications, reducing the need to provision Amazon EC2 capacity in advance. For example, clients can set a condition to add new Amazon EC2 instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the Amazon EC2 fleet goes above 70%; and similarly, clients can set a condition to remove Amazon EC2 instances in the same increments when CPU utilization falls below 10%.

Often, clients may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Clients can configure a cool down period for their Auto Scaling Group that tells Auto Scaling to wait for a specified period of time after taking an action before it evaluates the conditions again. Auto Scaling enables clients to run their Amazon EC2 fleet at optimal utilization.

Elastic Load Balancing: Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables clients to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until AWS restores the unhealthy instances. Clients can enable Elastic Load Balancing within a single AZ or across multiple zones for even more consistent application performance.

Amazon CloudWatch: Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications that clients run on AWS. Clients can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS database instances. CloudWatch also monitors custom metrics generated by applications and services and any log files a user's applications generate. Clients use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep application running smoothly. Amazon CloudWatch's metrics and alarms work together with Auto Scaling and Elastic Load Balancing to dynamically deploy new instances on-demand, as shown in Figure 9 below.

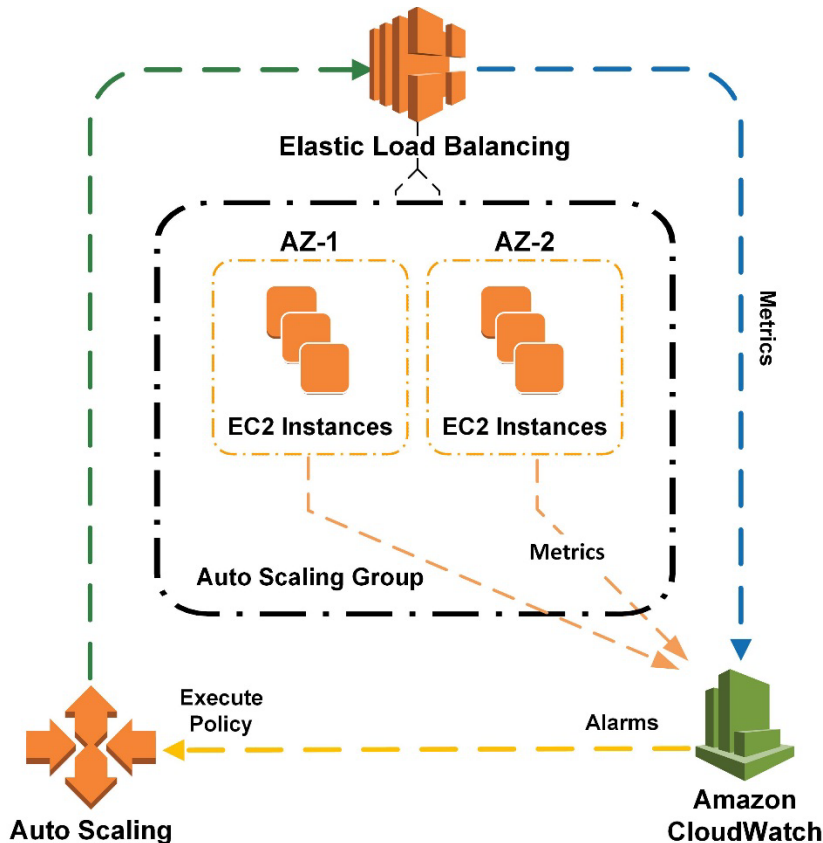


Figure 9: Amazon CloudWatch - Uses metrics and alarms to work together with Auto Scaling and Elastic Load Balancing to dynamically deploy new instances on-demand.

8.13 (E) CLOUD SECURITY ALLIANCE

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

- Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.**
- Completion of Exhibits 1 and 2 to Attachment B.**
- Completion of a CSA STAR Attestation, Certification, or Assessment.**
- Completion CSA STAR Continuous Monitoring.**

- CSA STAR Level 1: CSA STAR Self-Assessment:** AWS completed the CSA STAR Self-Assessment and published the results to the AWS website. This is the latest CAIQ (v3) released by the CSA.
- CSA Consensus Assessments Initiative Questionnaire:** CALIBRE has provided this questionnaire as a separate document to this submission with file name: CSA_Consensus_Assessments_Initiative_Questionnaire.pdf.
- CSA STAR Level 2: CSA STAR Attestation and Certification:** Per the CSA definitions, AWS aligns with the CSA STAR Attestation and Certification via the determinations in our third-party audits for SOC and ISO.

CSA STAR Level 2 Attestation is based on SOC 2. The SOC 2 report audit attests that a third-party auditor validated AWS's claims to confirm that AWS appropriately designed

their control objectives and that they are operating effectively. CSA STAR Level 2 Certification is based on ISO 27001:2005.

- d) **CSA STAR: Continuous Monitoring:** CALIBRE will address the CSA Continuous Monitoring requirements through the AWS Security by Design (SbD) program. SbD provides the control responsibility outlines, automation of security baselines, configuration of security, and the client audit of controls for AWS client infrastructure, operating systems, services, and applications running in AWS. This standardized, automated, prescriptive, and repeatable design can be deployed for common use cases, security standards and audit requirements across multiple workloads. AWS provides the tools necessary to meet the CSA STAR continuous monitoring requirements.

8.14 (E) SERVICE PROVISIONING

8.14.1 Emergency or Rush Services Implementation Process

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

CALIBRE will establish processes for handling implementation requests with each Purchasing Entity during the contract process, planning documents, or initial kickoff meeting. CALIBRE will recommend submitting implementation requests through our Service Desk. The Purchasing Entity will identify the authorized individuals to submit the requests. The implementation request would identify the criticality, required timelines, and the desire to process as an emergency or rush job. The Service Desk will prioritize the request and then route the request to AWS engineers for completion within the established SLAs and, as appropriate, within the requested timeline. In the event the request will incur additional costs, the Engineer will validate the request with the CALIBRE Contract Manager before moving forward.

The assigned CALIBRE engineer will provide the Purchasing Entity with a risk assessment and potential negative impacts that may occur as a result of the shortened implementation time. The engineer will perform the necessary backups and snapshots if the change could impact existing servers or databases. CALIBRE will discuss any outages or potential disruptions with the Purchasing Entity. Upon service completion, CALIBRE will provide the Purchasing Entity with an after action report.

8.14.2 Standard Lead-time for Provisioning Solutions

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

CALIBRE requires a minimum of 1 (one) business day lead-time for provisioning a solution, which is subject to negotiation with the Purchasing Entity for implementation. The lead-time assumes that the necessary configuration, network requirements, user access permissions, and other details are available to immediately begin provisioning work. Activities during this time may include setting up AWS organizations, designing AWS' IAM security structure, developing AWS tagging and resource groupings, and configuring Amazon Cloudwatch and Cloudtrail. CALIBRE will work with the Purchasing Entities to minimize lead times and validate the required information is available for quick deployments.

8.15 (E) BACK UP AND DISASTER PLAN

8.15.1 Legal Retention Periods

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

CALIBRE will work with purchasing entities to identify the legal retention periods and disposition instructions for the data and documents stored on the AWS cloud. CALIBRE will then establish the necessary scripts and processes into order to comply with these instructions. CALIBRE has extensive experience with records management software that will assist the purchasing entities in establishing file plans and the associated workflows to enforce the retention periods.

8.15.2 Known Inherent Disaster Recovery Risks

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

Amazon's infrastructure has a high-level of availability and provides users with the capability to deploy a resilient IT architecture. AWS designed its systems to tolerate system or hardware failures with minimal client impact. The primary risk associated with using AWS services is establishing and implementing the correct combination of services, capabilities and environments for an appropriate disaster recovery strategy. The disaster recovery strategy is dependent on a variety of factors for each solution such as criticality, robustness, data sensitivity, availability and cost. CALIBRE will work with each Purchasing Entity to mitigate this risk by developing the appropriate disaster recovery architecture as described below and then implement the associated services.

The AWS Cloud supports many popular disaster recovery architectures, ranging from "pilot light" environments that are ready to scale-up at a moment's notice to "hot standby" environments that enable rapid failover. All data centers are online and serving clients; no data center is "cold." In the case of a failure, automated processes move client data traffic away from the affected area. By distributing applications across multiple AWS AZs, users can remain resilient in the face of most failure modes, including natural disasters or system failures. Users can build highly resilient systems in the cloud by employing multiple instances in multiple AWS AZs and using data replication to achieve extremely high recovery time and RPOs. Users manage and test the backup and recovery of their information system that they build on the AWS infrastructure. Clients can use the AWS infrastructure to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. For more information, visit aws.amazon.com/disaster-recovery.

8.15.3 Infrastructure Support for Multiple Data Centers within the United States

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

CALIBRE's solution with AWS provides data centers throughout the United States. Each data center provides the full capabilities for operations including redundancy, failover capability, and the ability to run large scale applications independently. As described in section 8.8.2 Backup and Restore Services, AWS built their Cloud infrastructure around regions and AZs. AWS

regions provide multiple, physically separated and isolated AZs. They are connected with low-latency, high throughput, and highly redundant networking. These AZs offer AWS clients an easier and more effective way to design and operate applications and databases. Thus, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures.

AWS replicates critical system components across multiple AZs to provide high availability under normal circumstances and during disasters such as fires, tornadoes, or floods. AZs consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS AZ runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single AZ. AWS designs their data centers' electrical power systems to be fully redundant and maintainable without impact to operations. AWS data centers do not share common points of failure, such as generators, Uninterruptable Power Supply (UPS) units, and air conditioning across AZs.

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

Availability and Fault Tolerant Design: Amazon's infrastructure has a high -level of availability and provides users with the capability to deploy a resilient IT architecture. AWS designed its systems to tolerate system or hardware failures with minimal client impact.

AWS built data centers in clusters in various global regions. All data centers are online and serving clients; no data center is "cold." In case of failure, automated processes move client data traffic away from the affected area. AWS deploys core applications 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 users with the flexibility to place instances and store data within multiple geographic regions as well as across multiple AZs within each region. AWS designed each as an independent failure zone and physically separated them within typical metropolitan regions and in lower risk flood plains (flood zone categorization varies by Region). In addition to discrete UPS and on-site backup generation facilities, different grids from independent utilities feed each data center to further reduce single points of failure. AWS redundantly connected AZs to multiple tier-1 transit providers.

CALIBRE will support our clients to architect their AWS usage to take advantage of multiple regions and AZs. Distributing applications across multiple AZs provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures. However, users should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Only the client can proactively replicate data between regions, thus allowing clients with these types of data placement and privacy requirements the ability to establish compliant environments. Note that communications between regions is across the public Internet infrastructure. Therefore, the client should use the appropriate encryption methods to protect sensitive data.

8.16 (E) HOSTING AND PROVISIONING

8.17.1 Cloud Hosting Provisioning Processes

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, including cloud hosting provisioning, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Clients can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables clients to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS IAM users. The AWS Management Console supports all AWS regions and enables clients to provision resources across multiple regions.

Another option for cloud management in the AWS CLI is a unified tool used to provision and manage AWS Cloud services/servers on-demand. With just one tool to download and configure, clients can control multiple AWS resources from the CLI 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).

CALIBRE offers a cost optimized right sized architecture in AWS as cloud hosting provisioning decisions are made. Design decisions are sometimes directed by haste rather than data, and the temptation exists to overcompensate “just in case” rather than spend time benchmarking for the most cost-optimal deployment. This could lead to over-provisioned and under-optimized deployments. However, this is a reasonable choice when required to perform a “lift and shift” of resources from an on-premises environment to the cloud and then optimize afterwards. A cost optimization strategy up front allows for the realization of the economic benefits of the cloud more readily by ensuring a consistent adherence to best practices and avoiding unnecessary over provisioning. The following sections provide techniques and best practices for the initial and on-going cost optimization of the deployment and environment.

Right sizing is using the lowest cost resource that still meets the technical specifications of a workload. Right size iteratively by adjusting the size of resources to optimize for costs. Right sizing activities take into account the resources of a system and the attributes of each individual resource. Right sizing can be an iterative process, triggered by changes in usage patterns and external factors such as AWS price drops or new AWS resource types.

CALIBRE offers the knowledge skillset to leverage AWS APIs, SDKs, and features that allow resource changes as demands change. For example, we can perform on Amazon Elastic Compute Cloud (Amazon EC2) a stop-and-start to allow a change of instance size or instance type. We can restore a volume on Amazon Elastic Block Store (Amazon EBS) from a snapshot to a different volume type offering greater performance through increased input/output operations per second (IOPS) and/or throughput.

AWS has three options for EC2 Instances as the defined provisioning stack: On-Demand Instances, Spot Instances, and Reserved Instances. Then within these options, AWS EC2 has five different categories of server configurations (General Purpose, Computer Optimized, Memory Optimized, Accelerated Computing, and Storage Optimized) with three or more base configurations in each category and then various sets of options to select from for a server.

CALIBRE offers the Purchasing entity an analysis of the requirements for the solution and provides a recommendation on which of the three purchase models to employ based on cost optimization, availability, integrity and confidentiality of the solution.

8.17.2 Tool Sets

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).*

Deploying New Servers: The AWS CLI and the AWS console provide the client with the capability to provision new servers on-demand.

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Clients can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application.

AWS OpsWorks is a configuration management service that enables clients to configure and operate applications of all shapes and sizes using Chef. Clients can define the application's architecture and the specification of each component including package installation, software configuration, and resources such as storage. Clients can start from templates for common technologies like application servers and databases or build their own to perform any task that can be scripted. AWS OpsWorks includes automation to scale applications based on time or load and dynamic configuration to orchestrate changes as an environment scales.

AWS Marketplace is an online store that enables clients find, buy, and immediately start using the software and services they need to build products and run their businesses. AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. Visitors to AWS Marketplace can use 1-Click deployment to quickly launch pre-configured software and pay only for what they use, by the hour or month. AWS handles billing and payments, and software charges appear on clients' AWS bill.

Creating and Storing Server Images for Future Deployments: AWS provides the capability to store Images in an AMI, or snapshot. Clients can launch multiple instances from a single AMI when they need multiple instances with the same configuration. Clients can use different AMIs to launch instances when they need instances with different configurations. AMIs are categorized as either backed by Amazon EBS or backed by instance store. The former means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot. It means that the root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.

Securing Additional Storage Space: AWS provides EBS storage for EC2 instances that the client can create at will from the AWS API or console. Clients can create Amazon EBS Provisioned IOPS volumes that can store up to 16 TiB, and process up to 20,000 IOPS. Clients can also create Amazon EBS General Purpose volumes that can store up to 16 TiB, and process up to 10,000 IOPS. AWS designed these volumes for five 9s of availability and up to 320 megabytes per second of throughput when attached to EBS optimized instances. In addition clients can increase existing volumes in size up to the drive limits above if needed.

AWS also has object storage in the form of S3. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry. S3 provides robust security and compliance capabilities that meet even the most stringent regulatory requirements. It gives clients flexibility in the way they manage data for cost optimization, access control, and compliance. S3 provides query-in-place functionality, allowing clients to run powerful analytics directly on their data at rest in S3. With using AWS S3 for storage, the total volume of data and number of objects clients can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

Monitoring Tools for Authorized Personnel: Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that clients run on AWS. Clients 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 the client's applications and services and any log files their applications generate. Clients can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health and then use those insights to react and keep their application running smoothly.

AWS CloudTrail is a web service that records AWS API calls for a client's account and delivers log files to them. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service. With AWS CloudTrail, clients can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS Cloud services, such as AWS CloudFormation. The AWS API call history that AWS CloudTrail produces enables security analysis, resource change tracking, and compliance auditing.

AWS Trusted Advisor is an online resource to enable clients to reduce cost, increase performance, and improve security by optimizing their AWS environment. AWS Trusted Advisor provides real-time guidance to support clients with provisioning resources following AWS best practices. Trusted advisor analyzes the clients AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance and Service Limits.

Other Tools: AWS Service Catalog allows organizations to create and manage catalogs of AWS approved IT services. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows clients to centrally manage commonly deployed IT services, enables

them to achieve consistent governance, and assists them with compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

AWS has services available to assist application owners in building continuous integration and continuous delivery pipelines as well as configuration management.

AWS CodeCommit is a fully managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories. AWS CodeCommit eliminates the need to operate a source control system or worry about scaling its infrastructure. Clients can use AWS CodeCommit to securely store anything from source code to binaries, and it works seamlessly with existing Git tools.

AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. AWS CodePipeline builds, tests, and deploys a client's code every time there is a code change, based on the release process models they define. This enables clients to rapidly and reliably deliver features and updates. Clients can easily build an end-to-end solution by using our pre-built plugins for popular third-party services like GitHub or integrating custom plugins into any stage of the release process. With AWS CodePipeline, clients only pay for what they use. There are no upfront fees or long-term commitments.

AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, clients don't need to provision, manage, and scale their own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue. Clients can get started quickly by using prepackaged build environments, or they can create custom build environments that use their own build tools. With AWS CodeBuild, clients are charged by the minute for the compute resources they use.

AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for clients to rapidly release new features, enables them to avoid downtime during application deployment, and handles the complexity of updating their applications. Clients can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service also scales with infrastructure so clients can easily deploy to one instance or thousands.

AWS Config is a fully managed service that provides clients with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config Rules enables clients to create rules that automatically check the configuration of AWS resources recorded by AWS Config. With AWS Config, clients can discover existing and deleted AWS resources, determine their overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

AWS Systems Manager allows clients to centralize operational data from multiple AWS services and automate tasks across AWS resources. Clients can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, clients can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central

place to view and manage AWS resources, so clients can have complete visibility and control over their operations.

AWS provides a broad set of services that enable IT administrators, systems administrators, and developers more easily manage and monitor their resources. Using these fully managed services, clients can automatically provision, configure, and manage their AWS or on-premises resources at scale. Clients can also monitor infrastructure logs and metrics using real-time dashboards and alarms. AWS also enables clients monitor, track, and enforce compliance and security.

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

8.18.1 Testing and Training Periods

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

AWS offers one year free tier accounts for new clients with restricted use to gain experience on over 40 products with selected services and configurations. The core free offerings and preliminary restrictions are as follows:

- ▶ Amazon EC2: 750 hours per month on a EC2 Micro instances
- ▶ Amazon QuickSight: 1G of SPICE capacity
- ▶ Amazon RDS: 750 Hours per month of db.t2.micro database usage
- ▶ Amazon S3: 5 GB of standard storage
- ▶ AWS Lambda: 1 Million free requests per month

Other services and trial periods are available for selected services and varying time periods and restrictions. CALIBRE can also establish testing and training environments for purchasing entity use on a cost-reimbursement model. As an additional service, CALIBRE will offer to provide Purchasing Entities with training services and specialists for targeted training on services.

8.18.2 Test and/or Proof of Concept Environment

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.

CALIBRE is able to provide an AWS account as test and/or proof of concept environment for evaluation.

8.18.3 Training and Support at No Cost

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

AWS provides 33 10-minute tutorials at no cost as part of the AWS Free Tier. AWS also provides over 100 free digital courses for all levels of experience and a wide variety of subjects in 22 different categories.

8.18 E) INTEGRATION AND CUSTOMIZATION

8.19.1 Integrated Solutions

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.

CALIBRE will work with the Purchasing Entities to match the appropriate AWS services with the business requirements. AWS designed their product stack to be compatible with other AWS services such as EC2 servers using S3 storage. CALIBRE will develop the solution architecture and verify the integration of selected components. In the event external applications must be integrated with AWS components, AWS provides a SDK with documentation on the available Applicable Programming Interfaces (APIs) as REST interfaces.

8.19.2 Customized and personalized Solutions

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

CALIBRE begins every engagement with an assessment of client needs and methods to address these requirements. CALIBRE will propose the appropriate AWS stack to meet the needs and then, as necessary, provide recommendations on other tools, development, customization, processes or approaches to efficiently and effectively solve the Purchasing Entities issues. CALIBRE will present these options and then execute the agreed upon course of action.

Most of the AWS capabilities have flexible configuration options that address a wide variety of needs. For example, AWS EC2 has five different categories of server configurations (General Purpose, Computer Optimized, Memory Optimized, Accelerated Computing, and Storage Optimized) with three or more base configurations in each category and then various sets of options to select from for a server. This type of flexibility permeates throughout AWS services.

8.19 (E) MARKETING PLAN

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

CALIBRE, through our Growth Operations Division, offers extensive experience in public and federal sector marketing. Our dedicated team is responsible for developing and growing large contract vehicle offerings like NASPO ValuePoint. Growth Operations is committed to increasing orders sent and awarded through the NASPO ValuePoint contract through the lifespan of the vehicle. To accomplish this CALIBRE will develop digital and print marketing materials that showcase the benefits that the NASPO ValuePoint vehicle offers to participating entities in their cloud solution procurement efforts. In addition to producing new marketing materials, CALIBRE will incorporate NASPO ValuePoint language into existing marketing materials that are pertinent to our current set of corporate offerings including Big Data, Cloud Solutions, and Data Migration, and Data Analytics, just to name a few.

Upon award, CALIBRE will make the NASPO ValuePoint vehicle materials available through our corporate website and will include direct links to the NASPO ValuePoint site to allow for widest possible viewership. As part of our normal business procedures, CALIBRE will socialize the NASPO ValuePoint award and subsequent activities through focused press releases, and will post information on the vehicle to our established LinkedIn and Facebook pages. To allow for consistent communications, the Growth Operations will work to develop NASPO ValuePoint content and to facilitate an email marketing campaign.

To generate new leads, CALIBRE will use our focused marketing materials at the numerous tradeshow and events that we participate in. Additionally, CALIBRE will implement a lunch and learn program for our internal business development communities as well as for our

leadership teams to provide them a clear understanding of the value-added proposition of the NASPO ValuePoint vehicle for use at the numerous social networking, vendor programs, and public relations activities they participate in across the country.

CALIBRE's initial focus will be to leverage our relationships with our current state clients including those in Hawaii, Colorado, Maryland, and Washington to increase their use of our NASPO Master Agreement in their future cloud related IT activities. We will conduct an email and call campaign to establish business meetings with our existing client sets to provide them with an understanding of the NASPO ValuePoint vehicle. Following these meetings, CALIBRE will assist them with identifying potential opportunities to move new or existing work as allowable by their parent agencies and organizations to the NASPO ValuePoint vehicle.

8.20 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

CALIBRE provides a complete set of value-added services that span pre- and post-implementation. CALIBRE will work with potential Purchasing Entities to evaluate their needs and provide a proposal to meet their requirements. CALIBRE will provide the staff, capabilities and skills necessary to complete cloud engagements as we proposed. A partial list of value-added services CALIBRE provides includes:

► Requirements Analysis ► System Architecture ► System Design ► Software Development ► Testing ► Training	► User Documentation ► Security Assessments and Documentation ► Software installation and configuration ► System Integrations ► Network Architecture and Implementation	► Network and System Operations ► Service Desk Support ► Change Management ► Project and Program Management ► Enterprise Architecture
---	---	---

Purchasing Entity will address the entire scope of services for a successful implementation. CALIBRE will provide the Purchasing Entity with labor categories to draw upon and configure to meet pre- and post-implementation support required.

8.22 (E) SUPPORTING INFRASTRUCTURE

8.22.1 Solution Infrastructure

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

The Purchasing Entity requires no infrastructure to support CALIBRE's solution or deployment models.

8.22.2 Installation of New Infrastructure

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

The Purchasing Entity requires no infrastructure to support CALIBRE's solution or deployment models. If the Purchasing Entity chooses a hybrid cloud solution (a combination of mixture of AWS and Purchasing Entity on-premise requirement) and needs assistance with the installation and/or extension of their environment, CALIBRE is available to provide those services. In addition, CALIBRE can support the Purchasing Entities for the additional functions in a Community model such as establishing the connectivity and external permissions models.



**State of Utah, Division of Purchasing and
National Association of State Procurement
Officials (NASPO) ValuePoint**

**Cloud Solutions Request for Proposal (RPF)
Solicitation: SK18008**

**CALIBRE - Attachment 1: Sample Service Level
Agreements**

Prepared for:

Solomon Kingston
State Contract Analyst
State of Utah, Division of Purchasing
skingston@utah.gov
(801) 538-3228

July 6, 2018, 3:00 PM MT

CALIBRE Systems, Inc.

6354 Walker Lane
Metro Park, Suite 500
Alexandria, Virginia
22310-3252

p: 703.797.8500
f: 703.797.8501

www.calibresys.com

Amazon Compute Service Level Agreement

Last Updated February 12, 2018

This Amazon Compute Service Level Agreement (this “SLA”) is a policy governing the use of the Included Products and Services (listed below) by you or the entity you represent (“you”) under the terms of the AWS Customer Agreement (the “AWS Agreement”) between Amazon Web Services, Inc. and its affiliates (“AWS”, “us” or “we”) and you. This SLA applies separately to each account using the Included Products and Services. 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.

Included Products and Services

- ▶ Amazon Elastic Compute Cloud (Amazon EC2)
- ▶ Amazon Elastic Block Store (Amazon EBS)
- ▶ Amazon Elastic Container Service (Amazon ECS)
- ▶ Amazon Fargate for Amazon ECS (Amazon Fargate)

Service Commitment

AWS will use commercially reasonable efforts to make the Included Products and Services each available with a Monthly Uptime Percentage (defined below) of at least 99.99%, in each case during any monthly billing cycle (the “Service Commitment”). In the event any of the Included Products and Services do 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 any of the Included Products and Services, as applicable, was in the state of “Region Unavailable.” Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon Compute Services SLA Exclusion (defined below).
- ▶ “Availability Zone” and “AZ” mean an isolated location within a region identified by a letter identifier following the region code (e.g., us-west-1a).
- ▶ “Region Unavailable” and “Region Unavailability” mean:
 - For Regions with only one AZ, when that AZ and one AZ in any other Region, in which you are running an instance or task (one or more containers), as applicable, are concurrently “Unavailable” to you.
 - For all other Regions, when more than one AZ within the same Region, in which you are running an instance or task (one or more containers), as applicable, are concurrently “Unavailable” to you.
- ▶ “Unavailable” and “Unavailability” mean:
 - For Amazon EC2, Amazon ECS, or Amazon Fargate, when all of your running instances or running tasks, as applicable, 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 99.99% 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:

- I. the words “SLA Credit Request” in the subject line;
- II. the dates and times of each Unavailability incident that you are claiming;
- III. the affected EC2 instance IDs or the affected EBS volume IDs; 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 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.

SAMPLE

Amazon S3 Service Level Agreement

Last Updated April 4, 2018

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) and Amazon S3 One Zone – Infrequent Access (OneZone-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:

- ▶ The words “SLA Credit Request” in the subject line
- ▶ The dates and times of each incident of non-zero Error Rates that you are claiming
- ▶ Client 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.

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% 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:

- ▶ The words “SLA Credit Request” in the subject line
- ▶ The dates and times of each incident of non-zero Error Rates that you are claiming
- ▶ Client 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.

Amazon Route 53 Service Level Agreement

Last Updated December 1, 2016

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:

- ▶ The words “SLA Credit Request” in the subject line
- ▶ The dates and times of each period that Amazon Route 53 was not 100% Available that you are claiming
- ▶ Client 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 our reasonable control, including any force majeure event 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; 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” (collectively, the “Amazon Route 53 SLA Exclusions”). 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.

Amazon RDS Service Level Agreement

Last Updated March 25, 2016

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).
- ▶ "Multi-AZ instance" means an Amazon RDS for MySQL, MariaDB, 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:

- ▶ The words "SLA Credit Request" in the subject line
- ▶ The dates and times of each Unavailability incident you are claiming
- ▶ The DB Instance IDs and the AWS Regions of the affected Multi-AZ instances
- ▶ Client 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:

- ▶ Result from a suspension described in Section 6.1 of the AWS Agreement
- ▶ 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
- ▶ 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.)
- ▶ Result from instances belonging to the Micro DB instance class or other instance classes which have similar CPU and memory resource limitations
- ▶ 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.)
- ▶ Caused by underlying database engine software that lead to repeated database crashes or an inoperable database instance
- ▶ Result in long recovery time due to insufficient IO capacity for your database workload
- ▶ 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)
- ▶ Result from any maintenance as provided for pursuant to the AWS Agreement

- ▶ Arise 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.

SAMPLE

AWS Shield Advanced Service Level Agreement

Last Updated December 1, 2016

This AWS Shield Advanced Service Level Agreement (“SLA”) is a policy governing your subscription to AWS Shield Advanced 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 subscribed to AWS Shield Advanced. 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

For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, AWS will use commercially reasonable efforts to prevent those resources from failing to meet any service commitments specified in the Amazon CloudFront Service Level Agreement or Route 53 Service Level Agreement as a result of any denial-of-service attack covered by AWS Shield Advanced (the “Service Commitment”). In the event AWS Shield Advanced does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below. For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, a denial-of-service attack covered by AWS Shield Advanced will not constitute an Amazon CloudFront SLA Exclusion or Amazon Route 53 SLA Exclusion (as defined in the Amazon CloudFront Service Level Agreement and the Amazon Route 53 Service Level Agreement, respectively) with respect to a failure to meet any service commitments specified in the Amazon CloudFront Service Level Agreement or Route 53 Service Level Agreement.

Service Credits

For each 24-hour period (Coordinated Universal Time) in which Amazon CloudFront or Amazon Route 53 experienced an availability interruption that contributed to AWS Shield Advanced not meeting the Service Commitment you are entitled to a “Service Credit” in an amount equal to the average daily charges for AWS Shield Advanced for the monthly billing cycle in which the Service Commitment failure occurred. We will apply any Service Credits only against future AWS Shield Advanced 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 Service Commitment failure occurred. Service Credits will not entitle you to any refund or other payment from AWS. Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement (including the Amazon CloudFront Service Level Agreement or Amazon Route 53 Service Level Agreement), your sole and exclusive remedy for any unavailability of the AWS resources designated by you for protection by AWS Shield Advanced 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:

- ▶ the words “SLA Credit Request” in the subject line;
- ▶ the dates and times of each incident of availability interruption that you are claiming; and
- ▶ Client request logs that document the errors and corroborate your claimed availability interruption (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the failure to meet the Service Commitment 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.

AWS PUBLIC SECTOR ACCESS POLICY

(Last Updated April 2, 2018)

This AWS Public Sector Access Policy (“**Access Policy**”) is hereby made a part of the agreement (the “**Agreement**”) between [____INSERT END CUSTOMER NAME____] (“**Customer**”) and [____INSERT SOLUTION PROVIDER NAME____] (“**Solution Provider**”) regarding Customer’s use of and access to the AWS Services via the AWS accounts provided to Customer by Provider (“**Solution Provider Accounts**”). Section 7 contains definitions of capitalized terms.

1. Scope. This Access Policy is not an agreement with Amazon Web Services, Inc. (“**AWS**”). It sets out the rules, conditions, and restrictions that apply to Customer’s use of the AWS Services under Solution Provider Accounts where (1) Customer does not have an AWS Services Agreement with AWS; or (2) if Customer does have an AWS Services Agreement with AWS, Solution Provider has not designated it to AWS as Customer’s own account under the AWS Solution Provider Program.

2. Use of the Services.

2.1 Generally. Solution Provider gives Customer access to the AWS Services via Solution Provider Accounts, and Customer’s use of and access to the AWS Services is governed by the Agreement and this Access Policy. Contractual commitments by AWS to Solution Provider (for example, service level agreements) do not apply as between Customer and AWS. Customer must look solely to Solution Provider under this Agreement regarding any claims or damages relating to, or arising out of, the AWS Services. Solution Provider is not an agent of AWS and is not acting on behalf of AWS, and Customer is not a third party beneficiary of any agreement between Solution Provider and AWS.

2.2 Disclaimers; Limitations on AWS Liability. THE AWS SERVICES, AWS CONTENT, AND THIRD-PARTY CONTENT ARE PROVIDED “AS IS.” EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, NEITHER AWS, NOR SOLUTION PROVIDER ON BEHALF OF AWS, MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT. AWS DISCLAIMS ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (a) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (c) THAT THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (d) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST, ALTERED, OR DAMAGED. AWS WILL NOT BE LIABLE TO CUSTOMER FOR ANY DAMAGES OF ANY KIND (INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, DAMAGES FOR LOST PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA, THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY CUSTOMER IN CONNECTION WITH CUSTOMER’S USE OF THE AWS SERVICES, AWS CONTENT, OR THIRD-PARTY CONTENT) ARISING IN CONNECTION WITH, OR RELATED TO, CUSTOMER’S INABILITY TO USE THE AWS SERVICES, INCLUDING AS A RESULT OF ANY TERMINATION OR SUSPENSION OF SOLUTION PROVIDER ACCOUNTS UNDER ANY AGREEMENT BETWEEN AWS AND SOLUTION PROVIDER, DISCONTINUATION OR DOWNTIME OF AWS SERVICES, OR ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ACCOUNT CONTENT.

2.3 Account Keys. Solution Provider may provide Customer with AWS account keys which will allow Customer to directly access the AWS Services via Solution Provider Accounts. AWS is not responsible to Customer for any activities that occur under these account keys, regardless of whether the activities are undertaken by Customer, Solution Provider, or a third party (including Customer employees, contractors or agents) and AWS is not responsible to Customer for unauthorized access to Solution Provider Accounts.

2.4 Third-Party Content. Through the use of the AWS Services or the AWS Site, Customer may have access to Third-Party Content, which is made available directly to Customer by other entities or individuals under separate terms and conditions, including separate fees and charges. Customer’s use of any Third-Party Content is at its sole risk.

2.5 AWS Services Policies. All access to and use of AWS Services is subject to the AWS Services Policies. (Notwithstanding anything in the Acceptable Use Policy and AWS Service Terms, these two AWS Services Policies are not separate agreements between Customer and AWS.)

2.6 Customer Responsibilities. Unless otherwise agreed by Solution Provider, Customer is solely responsible for the development, content, operation, maintenance, and use of Account Content in Solution Provider Accounts, including (a) the technical operation of AWS Services in connection with Account Content; (b) compliance of Account Content with the AWS Services Policies and applicable law; (c) any action Customer permits, assists, or facilitates any other person or entity to take under Solution Provider Accounts; and (d) use of AWS Services or Account Content by End Users under Solution Provider Accounts (and ensuring that End Users comply with Customer obligations under this Access Policy). If Customer becomes aware of any violation of its obligations under this Access Policy caused by itself or an End User, Customer will immediately terminate such End User's access to Account Content and the AWS Services by such End User. Unless otherwise agreed by Solution Provider, Customer is solely responsible for properly configuring and using the AWS Services and otherwise taking appropriate action to secure, protect, and backup Solution Provider Accounts and Account Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Account Content from unauthorized access and routinely archiving Account Content.

3. AWS Services Interruption. AWS may suspend the Solution Provider Accounts used by Customer to access the AWS Services immediately if AWS determines Customer's or an End User's use of the AWS Services (i) violates the AWS Services Policies; (ii) poses a security risk to the AWS Services or any other AWS customer, (iii) may harm AWS systems or the systems or Content of any other AWS customer; or (iv) may subject AWS to liability as a result of any of the foregoing. We will provide notice of any suspension to Solution Provider, who is solely responsible for providing any notices to Customer under the Agreement. Nothing in this Section 3 will operate to limit Customer's rights or remedies otherwise available to Customer against Solution Provider under the Agreement or applicable law.

4. Transition of Solution Provider Accounts. Except as otherwise provided by law or the Agreement, a transition of Solution Provider Accounts from Solution Provider to a third party (or directly to AWS) requires advance written consent by Solution Provider (which Solution Provider must also obtain from AWS). Customer agrees to cooperate with Solution Provider in transitioning Solution Provider Accounts, and to provide all appropriate information and take all appropriate action necessary to facilitate such transition. In any case, absent prior authorization by AWS, Customer may not transfer Solution Provider Accounts to other providers that are not authorized to resell AWS Services.

5. Proprietary Rights

5.1 Generally. AWS or its licensors own all right, title, and interest in and to the AWS Services, and all related technology and intellectual property rights. Customer (a) has the right to access and use the AWS Services under Solution Provider Accounts solely in accordance with this Access Policy and the Agreement, and (b) may copy and use the AWS Content provided by Solution Provider (or, as applicable, by AWS) solely in connection with Customer's permitted use of the AWS Services. Except as provided in this Section 5, Customer obtains no rights under this Access Policy from AWS, its affiliates, or Solution Provider to the AWS Services, the AWS Content, or Third-Party Content, including any related intellectual property rights. Some AWS Content and Third-Party Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, or other open source license. By using those materials, Customer is subject to such additional terms. Customer is solely responsible for securing any necessary approvals for the download and use of such materials.

5.2 Restrictions. Neither Customer nor any End User will use the AWS Services or AWS Content in any manner or for any purpose other than as expressly permitted by this Access Policy and the Agreement. Neither Customer nor any End User will, or will attempt to (a) modify, distribute, alter, tamper with, repair, or otherwise create derivative works of any AWS Content or Content included in the AWS Services (except to the extent Content included in the AWS Services is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the AWS Services or apply any other process or procedure to derive the source code of any software included in the AWS Services (except to the extent applicable

law doesn't allow this restriction), or (c) access or use the AWS Services in a way intended to avoid incurring fees or exceeding usage limits or quotas.

5.3 Suggestions. If Customer provides any Suggestions to AWS or its affiliates, AWS and its affiliates will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions and agrees to provide Customer and AWS any assistance required to document, perfect, and maintain AWS's rights in the Suggestions.

5.4 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the AWS Services are provided (as applicable) as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the AWS Services. If Customer is using the AWS Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Customer will immediately discontinue its use of the AWS Services (including any AWS Content).

6. Representations and Warranties. Customer represents and warrants to Solution Provider that (a) Customer's and its End Users' use of the AWS Services (including any use by its employees, personnel, and (except for Solution Provider) contractors) will not violate this Access Policy, including the AWS Services Policies; (b) Customer or its licensors own all right, title, and interest in and to Account Content; (c) Account Content (including the use, development, design, production, advertising, or marketing of Account Content) or the combination of Account Content with other applications, Content, or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) Customer's use of the AWS Services will not cause harm to any End User.

7. Definitions.

"Account Content" means Content that Customer or any End User (a) runs on the AWS Services, (b) causes to interface with the AWS Services, or (c) uploads to the AWS Services or otherwise transfer, process, use or store in connection with the AWS Services.

"AWS Content" means Content AWS makes available (either directly or indirectly) in connection with the AWS Services or on the AWS Site to allow or facilitate access to and use of the AWS Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the AWS Services.

"AWS Services" means, collectively or individually (as applicable), the web services made commercially available by us to Solution Provider for use under this Access Policy, including (as applicable) those web services described in the AWS Service Terms.

"AWS Services Agreement" means the AWS Customer Agreement at <http://aws.amazon.com/agreement>, or other written agreement by and between AWS and Customer (if any) governing Customer's access to and use of the AWS Services.

"AWS Services Policies" means the following provisions (uses of the pronoun "you" shall refer to Customer):

- *AWS Acceptable Use Policy*, located at <http://aws.amazon.com/aup> (as it may be updated by AWS from time to time), which describes prohibited uses of the AWS Services and the AWS Site;
- *AWS Service Terms*, located at <http://aws.amazon.com/serviceterms> (as they may be updated by AWS from time to time), which include the rights and restrictions for particular AWS Services;
- *AWS Site Terms*, located at <http://aws.amazon.com/terms/> (as they may be updated by AWS from time to time), which govern the use of the AWS Site; and
- All restrictions described in the AWS Content and on the AWS Site.

"AWS Site" means <http://aws.amazon.com> and any successor or related site designated by AWS.

"Content" means software (including machine images), data, text, audio, video or images.

“Documentation” means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at <http://aws.amazon.com/documentation>, as such documentation may be updated by us from time to time.

“End Customer Account” means an AWS account designated as such under the AWS Solution Provider Program, through which AWS Services are provided by Solution Provider to Customer, and in connection with which AWS and Customer have an AWS Services Agreement.

“End User” means any individual or entity that directly or indirectly through another user: (a) accesses or uses Account Content; or (b) otherwise accesses or uses the AWS Services under Solution Provider Accounts. The term “End User” does not include individuals or entities when they are accessing or using the AWS Services or any Content under their own AWS account, rather than Solution Provider Accounts.

“Solution Provider Accounts” means Solution Provider’s AWS accounts through which AWS Services are provided by Solution Provider to Customer.

“Suggestions” means all suggested improvements to the AWS Services or AWS Content that Customer provides to AWS or its affiliates.

“Third-Party Content” means Content made available to Customer by any third party on the AWS Site or in conjunction with the AWS Services.