Contract # AR2488

STATE OF UTAH COOPERATIVE CONTRACT

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

SHI International Corp.
Name
290 Davidson Avenue
Address
Somerset NJ 08873
City State Zip

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

Contact Person: Nick Grappone Phone: 732-564-8189 Email: Nick_grappone@shi.com
Vendor #33386DD Commodity Code #920-05

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

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

4. CONTRACT PERIOD: Effective Date: 09/30/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Pursuant to Solicitation #CH16012, Contractor must re-certify its qualifications each year.

5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) 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.

6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
ATTACHMENT E: Service Provider Terms and Conditions

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

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

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

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

CONTRACTOR

Natalie Slowik 2/2/17
Contractor's signature Date

Natalie Slowik, Director of Response Team
Type or Print Name and Title

STATE

for 2.3.2017
Director, Division of Purchasing Date

Spencer Hall	801-538-3307	801-538-3882	spencerh@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions and the cloud service provider service terms;
(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. Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A, except for conflicts between the Attachment A Exhibits and Attachment E, which in that event, Attachment E will prevail. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

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

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

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

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

[1] A Sample Participating Addendum will be published after the contracts have been awarded.

[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Each party 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 the other Party or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by the receiving Party 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 the receiving Party) publicly known; (2) is furnished by the disclosing Party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving Party'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 the disclosing Party without the obligation of confidentiality, (5) is disclosed with the written consent of the disclosing Party or; (6) is independently developed by employees, agents or subcontractors of the receiving Party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Each Party 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, the party claiming default shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the party in default 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 the party in default is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the party in default 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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment for the portion of the nonconforming Service at issue 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.

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 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. Contractor's duties under this provision are dependent on the indemnified party giving Contractor (1) prompt written notice of such third party claim and (2) sole authority to defend or settle the claim.

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 Service 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 claim based on:

(a) Contractor's compliance with Participating Entity/Purchasing Entity's designs, specifications or instructions; or

(b) Contractor's use of technical information or technology provided by the Participating Entity/Purchasing Entity; or

(c) non-Contractor software, modifications a Participating Entity/Purchasing Entity makes to, or any specifications or materials a Participating Entity/Purchasing Entity provides or makes available for a Service; or

(d) Participating Entity/Purchasing Entity's combination of the Service with a non-Contractor product, data or business process; or damages based on the use of a non-Contractor product, data or business Process; or

(e) Participating Entity/Purchasing Entity's use of either Contractor's trademark.

(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 Contractor reasonably believes that a Service may infringe or misappropriate a third party's intellectual property rights, Contractor will seek to (i) procure for Participating Entity/Purchasing Entity the rights to continue to use the Service or (ii) modify or replace it with a functional equivalent to make it non-infringing and notify Participating Entity/Purchasing Entity to discontinue use of the prior version, which Participating Entity/Purchasing Entity must do immediately. If the foregoing options are not commercially reasonable for Contractor, or if required by a valid judicial or government order, Contractor may terminate Participating Entity/Purchasing Entity's license or access rights in the Service.

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, if Contractor hosts this kind of data:

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

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

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

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

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

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

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

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

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

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

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

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

d. Contractor shall not begin providing Services without a valid Service Level

Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

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

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

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

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

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

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a

Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

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

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

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

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

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

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

21. Payment: Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Unless otherwise provided for in the service provider terms, 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: Unless otherwise provided in the service provider terms, 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.

Unless otherwise provided for in the service provider terms, 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: RESERVED

29. Title to License: 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 service provider 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. Unless otherwise provided for in the services terms in Attachment E, 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 must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all

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

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

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

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

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://www.naspo.org/WNCPO/Calculator.aspx. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

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

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

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

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

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

43. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity.

44. Limitation of Liability: Except as otherwise set forth in the Indemnification paragraphs above, the limit of liability shall be as follows:

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

b. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity’s satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

The limitation of liability in Section 44 will not apply to claims for bodily injury or death.

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Identification of Service Models Matrix

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Saas	X	X	X	**CA Technologies** CA Technologies provides SaaS solutions that help agencies from planning to development to software development to enabling online business with security. CA Technologies help jump start the IT process so that agencies can become more agile and manage their IT operations with more efficiency and lower cost. CA Technologies offers a portfolio of five different SaaS Applications to enable agencies to be thrive in the application economy. • Project Portfolio Management (CA PPM) • Agile Central • Application Synthetic Monitoring (CA ASM) • Application Performance Monitoring (CA APIM • Mobile Apps Analytics (CA MAA) **Microsoft Azure** Azure has connections to over 3000 SaaS based apps covering virtual machines, developer services, API applications, Office 365, Azure Active Directory application connectors, Web applications, data services

				and Microsoft Dynamics solutions via the Azure Marketplace.
IaaS	X	X	X	**AWS** • **Community cloud.** In addition to the AWS GovCloud, it is possible to create community clouds using AWS Dedicated Hosts and group network access controls so that only members of a designated community have access to cloud resources. • **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. • **Hybrid cloud.** Public and Community models can be combined. **Microsoft Azure** Azure has connections to over 3000 SaaS based apps covering virtual machines, developer services, API applications,Office 365, Azure Active Directory application connectors, Web applications, data services and Microsoft Dynamics solutions via the Azure Marketplace.
PaaS	X	X	X	**AWS** • **Community cloud.** In addition to the AWS GovCloud, it is possible to

				create community clouds using Dedicated Hosts and group network access controls so that only members of a designated community have access to cloud resources. • **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. • **Hybrid cloud.** Public and Community models can be combined. **Microsoft Azure** Azure has connections to over 3000 SaaS based apps covering virtual machines, developer services, API applications,Office 365, Azure Active Directory application connectors, Web applications, data services and Microsoft Dynamics solutions via the Azure Marketplace.

Attachment C – Cost Schedule

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

Software as a Service **Discount %** 1

Infrastructure as a Service **Discount %** 1

Platform as a Services **Discount %** 1

Value Added Services **Discount %** 1

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate $ 90-300
Remote Hourly Rate $ 90-300

Professional Services

- **Deployment Services**
  Onsite Hourly Rate $ 90-300
  Remote Hourly Rate $ 90-300
- **Consulting/Advisory Services**
  Onsite Hourly Rate $ 90-300
  Remote Hourly Rate $ 90-300
- **Architectural Design Services**
  Onsite Hourly Rate $ 90-300
  Remote Hourly Rate $ 90-300
- **Statement of Work Services**
  Onsite Hourly Rate $ 90-300
  Remote Hourly Rate $ 90-300

Partner Services

Onsite Hourly Rate $ 90-300
Remote Hourly Rate $ 90-300

Training Deployment Services

Onsite Hourly Rate $ 90-300
Online Hourly Rate $ 90-300

Please see the next page for additional information regarding SHI's proposed pricing to NASPO ValuePoint.

SaaS/IaaS/PaaS are all rapidly emerging technologies. As such, pricing products offered and pricing structure for those products can change rapidly. Currently SHI discounts for OEM's that provide this technology range greatly. In addition, in most cases these solutions are customized on a case by case basis and depend greatly on the current infrastructure, the workloads being considered for migration and the amount of expected growth. SHI is always trying to stay competitive and we will continually work to provide NASPO Participating Entities the highest discounts we are able to provide.

On the attached spreadsheet we provide an example of pricing for Microsoft O365 and Azure as well as Amazon Web Services. SHI can agree to a minimum discount of list minus 1% on all of the delivery models but in many cases may often be able to give more extensive discounts.

As it relates to Additional Value Added Services the same is true. The cloud environment is evolving and as it does the type and scope of service engagements and offerings change as well. The categories listed on the Cost Schedule can vary widely depending on the specific engagement as many of the solutions that will be procured through this contract will be usage based, meaning, NASPO Entities will be billed only for what they use in a specific month or quarter. Each partner has a different strategy for usage based billing. The Participating Entities dedicated SHI account teams will work with them to review and understand the various billing strategies associated with the solutions.

SHI has provided a range of hourly fees based on typical engagements that we deliver today. As service models develop we will work with NASPO to create a pricing structure that benefits the NASPO Participating entities.

Please see below for standard levels of service provider and actual hourly rates SHI would charge today.

Service	**NASPO Price/Hour**
Associate Consultant	$110
Consultant	$162
Solution Architect	$225
Sr. Solution Architect	$285
Program Engagement Manager	$93
Project Leader	$98
Project Manager	$135
Sr. Project Manager	$199

SHI would welcome the opportunity to discuss our price offering for NASPO in more detail. We are also open to other pricing models, should NASPO determine that another pricing model would best meet the need of your Participating Entities.

The State of Utah and NASPO ValuePoint

Cloud Solutions

RFP #CH16012

SHI International Corp.

290 Davidson Avenue, Somerset, NJ 08873 • 888-764-8888 • SHI.com

March 10, 2016

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

Dear NASPO ValuePoint and the State of Utah

SHI is pleased to provide the following response to your recent request for proposal. Per the bid request, our cover letter includes the following required statements.

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

SHI Response:

SHI acknowledges that negotiations of additional terms and administrative fees may be required by Participating Entities.

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

SHI Response:

SHI is responsible for writing this proposal led by Senior Director Public Sector - Denise Verdicchio, Director of West Region Public Sector - Alison Turner, Senior Contract Manager – Natalie Slowik, and Public Program Manager Meghan Flisakowski. In addition to the SHI team, we used resources available to us from the partners we are presenting as part of our response.

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

SHI Response:

SHI is currently in good standing with Federal and State procurement and non-procurement programs.

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

SHI Response:

SHI acknowledges the 0.25% Administrative Fee for total sales under the Master Agreement associated with this NASPO ValuePoint RFP as well as any fees from the Participating Entities.

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

SHI Response:

SHI will partner with OEM's who provide each of the service/deployment models NASPO is requesting. Our proposed service models are IaaS and PaaS, each deployed in either Community, Public or Hybrid models.

As the technology and customer's needs in these categories are constantly emerging, it is SHI's intention to continually review and identify new partners and solutions that may be appropriate for the NASPO ValuePoint Cloud contract.

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

SHI Response:

Our proposed IaaS and PaaS cloud offers have the ability to store and secure Low, Moderate and High Risk data in conformance with FIPS designations.

Table of Contents

5 MANDATORY MINIMUM REQUIREMENTS

5.1 SIGNATURE PAGE

The signature page has been completed online per bid instructions.

5.2 COVER LETTER

Per bid requirements the information requested can be found in SHI's cover letter found previously in this RFP response document.

5.3 ACKNOWLEDGEMENT OF AMENDMENTS

Per bid requirement, SHI has acknowledged the amendments associated with this RFP.

5.4 Executive Summary

SHI International Corp. is pleased to submit our response to the NASPO ValuePoint Solicitation CH16012 for Cloud Solutions. SHI has been in business for over 26 years as an IT Solutions provider. We appreciate our strong partnership with NASPO ValuePoint, and we look forward to driving even more benefits to NASPO ValuePoint Participating Entities through this Cloud Solutions agreement. Our response intends to establish the basis for an initial Cloud Solutions contract and create a path by which we will continue to meet NASPO ValuePoint's evolving needs in this rapidly changing marketplace.

As with the NASPO ValuePoint Software Value Added Reseller contract, SHI intends to approach the Cloud Solutions contract with the same degree of dedication and commitment. This commitment starts with the dedicated account teams for State and Local Government and Education as we realize that it is important for these teams to focus your unique needs and requirements. This commitment is evident not only by the tenure of our sales teams but also our desire to grow our account team so we can continue to bring more dedicated support to our the SLED customers.

We realize though that it takes more than just a great account team. SHI's e-Procurement systems are highly advanced and customized for our customers. Our quoting, ordering, tracking, and reporting capabilities are all customizable to help simplify our customers' processes.

In addition, SHI's pricing methodology is competitive and stands the test of time. We understand that government entities need to identify cost savings wherever possible. SHI's proposal not only offers a competitive price point, but also provides additional opportunities to assist customers with real savings and help you to achieve best value in your procurements.

Why SHI for Cloud Solutions?

At SHI, we understand that one size does not fit all; each customer has different objectives and procurement requirements. The processes requirements, system workflow and options, and the information to be collected with a requisition all vary widely from customer to customer. In fact, we have found they often vary within a customer, as different business units and organizations may have differences in product selection or preferred systems solutions.

SHI has the ability to assess what the client is trying to accomplish and map the best technology to that environment. In a market where technology is rapidly changing, we bring further value by offering the ability to add partners and solutions as they emerge. Our goal will be to work in partnership with NASPO ValuePoint and expand this contract to include all of these offerings so we can provide end to end solutions for the member community. NASPO ValuePoint customer will have access to our broad product offering including cloud products such as:

- Microsoft Office 365
- Box
- Adobe Creative Cloud
- AWS
- CA Technologies

Rather than attempt to force multiple customers into a single support model, SHI provides systems and services that adapt and scale to the customer's varying needs. Our Public Sector Account Executives provide customized and specialized support for their local customers, ensuring SHI is meeting their requirements, while upholding the terms of the NASPO ValuePoint agreement.

SHI understands that our customers need to become faster and more agile as their “customers” demand more capabilities and speed to completion from their internal IT organizations. When deciding upon a cloud based solution it is also important that organizations understand the true cost associated with subscribing to a service over traditional on premise procurements. Lastly, evaluating customer workloads and how that should factor into the decision making process for cloud services is imperative. The SHI sales team works in concert with SHI product specialists and with our cloud partners to help our clients procure, configure, migrate, and make-ready all the components needed to deploy. We then stay proactively involved to maintain our clients’ environment. As hybrid and cloud based environments become the norm, NASPO ValuePoint customers will gain valuable perspective when they align with a partner that was not born in the cloud. SHI brings the unique ability to consult and execute across cloud and traditional on-premise environments.

SHI has helped our customers acquire over $1B of cloud based services and technology. We have helped these customers recognize savings by selecting and right sizing the right cloud service platform. We look forward to doing the same for NASPO ValuePoint customers.

SHI has demonstrated that we are a top partner for NASPO ValuePoint Participating States. We are confident in our ability to meet and exceed your expectations and requirements under this contract. Per bid requirements we have provided a separate section regarding the Master Agreement Terms and Conditions of this RFP. Our partners have provided additional comments and SHI agrees to work with NASPO ValuePoint in the review and discussion of these terms.

SHI would welcome the opportunity to discuss our proposal with you in more detail. We hope you find our proposal compelling, based upon the elements of this offer and also based upon the strong relationship that SHI has developed with NASPO ValuePoint. We are confident in our ability to provide excellent support to NASPO ValuePoint and each Participating State under the Cloud Solutions contract, and we look forward to working with you!

5.5 GENERAL REQUIREMENTS

5.5.1

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

SHI Response:

SHI acknowledges and will provide a Usage Report Administrator who is responsible for the quarterly sales reporting as agreed to in the Master Agreement Terms and Conditions and any agreed to Participating Addendums.

5.5.2

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

SHI Response:

SHI acknowledges and agrees to work with SciQuest (and any authorized agent or successor entity to SciQuest).

5.5.3

- *Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment1. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or to submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both documents.*

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. For this response we have included three partners, AWS, CA Technologies, and Microsoft Azure/O365. Each of these partners have reviewed the requirements associated with this RFP and provided the information they believe is applicable and necessary.

[1] CSA STAR Self-Assessment documents the security controls provided by an Offeror's offerings, thereby helping Purchasing Entities assess the security of an Offeror, if awarded a Master Agreement, they currently use or are considering using.

5.5.4

- *Offeror, as part of its proposal, must provide a sample of its Service Level Agreement[2], which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.*

SHI Response:

SHI understands the importance of clearly defined SLAs to NASPO Participating Entities. We have included SLA examples for the partners that we are responding with and will continue to provide NASPO this information as we add partners/products over the life of the contract. Additional information regarding SLAs of the proposed solutions can be found in our response to 8.10.2.

5.7 Recertification Of Mandatory Minimums And Technical Specifications

- *Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.*

SHI Response:

SHI acknowledges this request and agrees to annually certify with the Lead State the technical capabilities identified in this response.

[2] SLAs can vary depending on the cloud service being procured as well as the individual ordering activity, and the Lead State does not expect to require a single SLA to all cloud solutions being proposed under the RFP. Additionally, by submitting a sample the Lead State does not agree to its terms and you understand that a Purchasing Entity may revise the SLA to conform to the requirements of its laws.

6 Business Information

6.1 Business Profile

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

SHI Response:

Founded in 1989, SHI International Corp. is a global provider of technology products and services. Over the past 20 years SHI has transformed itself from a $1 million "software-only" regional reseller into a global, full lifecycle provider of technology, services and solutions. Our ability to adjust as technology does allows us to keep pace with what is relevant and important to our customers including cloud and on-premise solutions. SHI is ranked 15th among CRN's Solution Provider 500 list of North American IT solution providers. With over 3,500 employees worldwide, SHI is the largest Minority and Woman Owned Business Enterprise (MWBE) in the U.S. SHI does not provide retention rate per individual teams but as a company we have an average 78% retention rate.

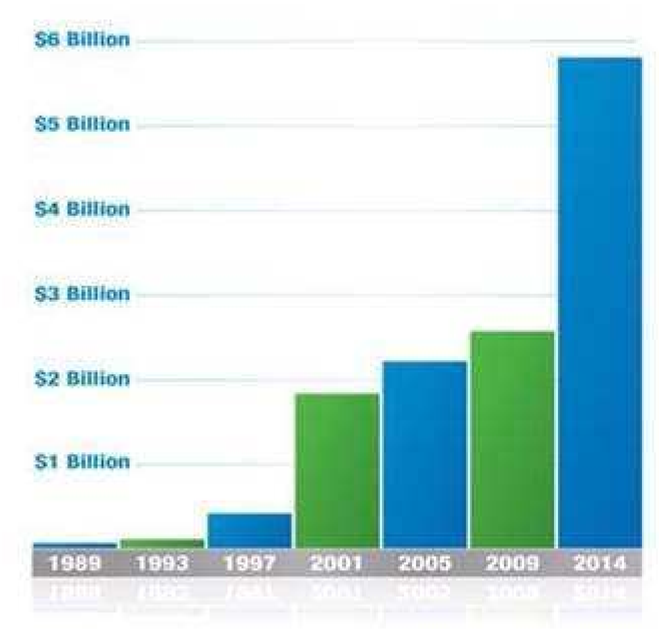
Driven by the industry's most experienced and stable sales force and backed by software volume licensing experts, hardware procurement specialists, and certified IT services professionals, SHI delivers custom IT solutions to Corporate, Enterprise, Public Sector, and Academic customers. Providing world class support to more than 14,000 customers, SHI continues to grow our customer base and maintain our customer loyalty with 99% retention.

SHI International Corp., headquartered in Somerset, New Jersey and has 30+ offices across the United States, Canada, United Kingdom, Germany, France and Hong Kong. SHI has a team of 3,500, with more than 900 employees in Texas, and more than 1,500 in New Jersey. Within the Public Sector, we currently have 95 dedicated field representatives and intend to continue growing the team. We have remained under the same ownership since 1989 and most Vice Presidents and Managers have been with SHI for more than 15 years.

We value our relationships with publishing and manufacturing partners who create products and solutions for you. Across a majority of product specific entities, we have forged longstanding alliances with their top manufacturers (in the spirit of our vendor agnostic approach) and their management and support teams, so that we might better serve the needs of our customers. Our sales and support teams also attend seminars, training, and customer facing events in support of new technology solutions and customer goals.

SHI has been supporting customers in their acquisition of cloud technology since its emergence on the market when traditional software partners began offering SaaS versions of their products. SHI immediately began to support this emerging technology for our customers. This has grown to include PaaS and Iaas. We have hired dedicated support teams internally to help address the specific needs of our customers when looking at any type of cloud based technology as these can vary greatly from on premise solutions.   We help analyze their current environment and infrastructure, address their business needs and desired outcomes and the help to develop a cloud ready strategy that not only accounts for now but will also scale to meet future needs.   SHI has helped our customers acquire over $1B of cloud based services and technology. We have helped these customers recognize savings by selecting and right sizing the right cloud service platform. Additional information on customers who have worked with SHI on similar solutions can be found in our response to question, 6.2.

For 2015 SHI reported earnings of $6.8B, which demonstrates 14% growth over 2014. SHI has a financially strong and stable business model that has proven itself over time. Providing a compelling value to our entire customer base, SHI is able to offer the lowest gross margin of our top 4 competitors, while at the same time maintaining our profitability with the lowest overhead cost structure in the industry. SHI has remained a privately-held company under the same owner since 1989. As privately held company we do not release all financial information but would be happy to discuss in more detail with NASPO ValuePoint if needed.



6.2 Scope of Experience

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

SHI Response:

SHI has been supporting customers in their acquisition of cloud technology since its emergence on the market when traditional software partners began offering SaaS versions of their products. SHI immediately began to support this emerging technology for our customers. A few examples of these customers include:

State of Florida

Microsoft, Symantec, VMware Contracts
Approximately $45 million in cloud sales in the last 2 years

State of Alabama

Microsoft, Symantec, VMware Contracts
Approximately $15 million in cloud sales in the last 2 years

City of Baltimore MD

AWS
Approximately $12 thousand in cloud sales in the last 2 years

Commonwealth of Kentucky Office of Technology

Microsoft Azure
Quarterly Billing: $31,648 Office 365 Users: 29000

Commonwealth of Kentucky Department of Education (KETS)

Microsoft Azure
Quarterly Billing: $32,751 Office 365 Users: 1,250,000

6.3 Financials

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

SHI Response:

SHI remains an operationally and financially stable company. We have remained under the same ownership since 1989 and most Vice Presidents and Managers have been with SHI more than 15 years.

SHI D&B Number is: 61-142-9481

CREDIT RATING:

SHI's D&B Rating: 5A3 (Credit Score)

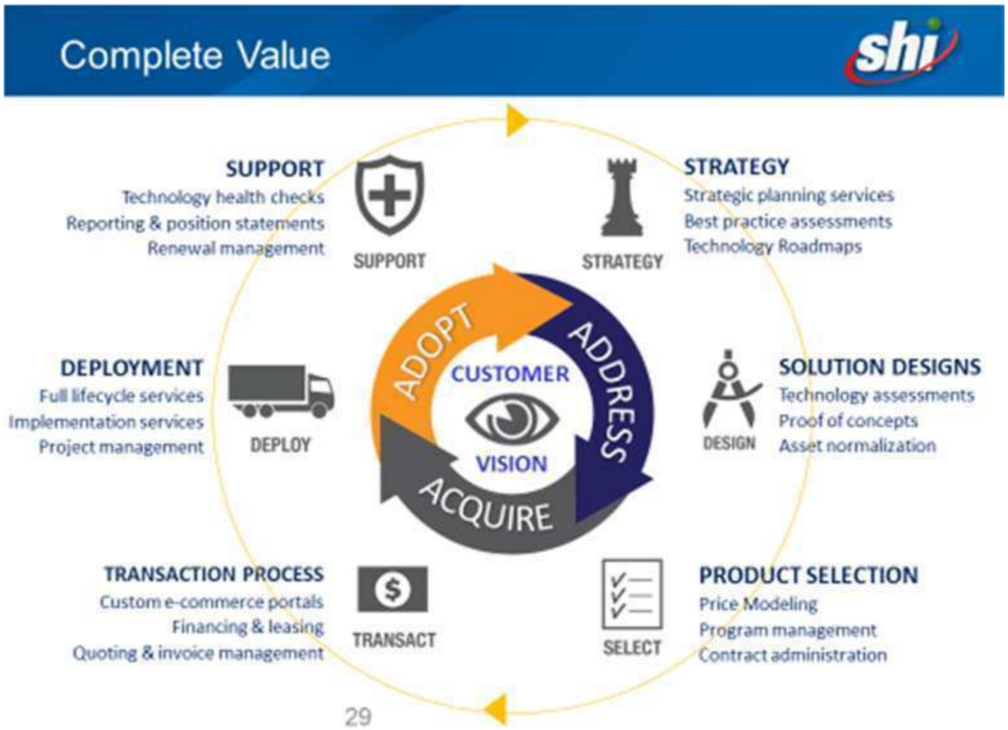
6.4 General Information

6.4.1

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

SHI Response:

SHI understands that in order to bring the right solution to the customer, we need to first understand their vision. Once we understand what they are trying to accomplish, our pre-sales engineers help design a strategy that is suitable to their environment today, and that will scale to meet their future needs. This approach might include conducting assessments of the customer's current environment or proof of concept for a potential solution. When the customer is ready to move forward, SHI will help to ensure that the customer is procuring those products using the most advantageous pricing programs and at the most aggressive possible cost. We then follow through with deployment services and support to ensure that the solution the customer procured is working as expected.



As cloud offerings continue to transition from IT marketing buzzwords to viable IT solutions, SHI continues to adjust our value-added solutions to support customers at every stage of cloud adoption.

Whether you're still assessing how the cloud fits into your environment, are split between some already deployed cloud applications/infrastructure and some legacy IT solutions, or are already 100% in the cloud, SHI can help.

Utilizing cloud solutions requires coordinating both business and technical resources across multiple business units. Since each business owner has different goals, SHI provides the tools, processes, and expertise to ensure your organization's usage of cloud computing is available, compliant, secure, makes good business sense and is seamless to end-users.

To support your cloud efforts, SHI offers:

- **Assess** – We offer both vendor-agnostic and manufacturer-specific assessments to guide you through every step of moving to the cloud.
- **Deploy** – We help you get your cloud up and running with an array of SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service), and PaaS (Platform-as-a-Service) solutions.
- **Maintain** – We make managing your cloud easy and predictable by assisting with reporting, billing, support contract management, and more.

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from Amazon Web Services (AWS), Microsoft Azure and O365, and CA Technologies as well additional service offerings from our partner Ascent Innovations.

AWS Response:

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

- **Pace of Innovation:** AWS's pace of innovation is funded and sustained through our economies of scale and commitment to delivering the products and services that matter most to our customers. Our approach to product development and delivery is fundamentally different than that of other Cloud Service Providers (CSPs). We have decentralized, autonomous development teams that work directly with customers. They are empowered to autonomously develop and launch new features based on what they learn from interactions with both commercial and public sector customers. AWS's continual innovation ensures that customers maintain state-of-the-art IT infrastructure without having to make recapitalization investments. As of January 1, 2016, AWS has launched a total of 1,896 new services or major features since inception in 2006 (including 516 in 2014 and 722 in 2015). According to the Gartner, Inc. 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide, "AWS is a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market."
- **Service Breadth and Depth:** AWS offers the broadest set of global compute, storage, networking, database, analytics, application, deployment, management, and mobile services that help organizations move faster, lower IT costs, and scale applications. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 50 services that serve over one million active customers in more than 190 countries through our 12 regions, 32 Availability Zones, and 54 Edge Locations. Gartner Inc. reported in its 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report that AWS "has the richest array of IaaS features," "continues to rapidly expand its service offerings and offer higher-level solutions," and has "over 10 times more cloud IaaS compute capacity in use than the aggregate total of the other 14 providers in this Magic Quadrant."
- **Partner and Software Ecosystem:** According to the Gartner, Inc. 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report, AWS has attracted "a very large technology partner ecosystem that includes software vendors that have licensed and packaged their software to run on AWS, as well as many vendors that have integrated their software with AWS capabilities. It also has an extensive network of partners that provide application development expertise, managed services, and professional services such as data center migration." AWS has thousands of organizations in the AWS Partner Network (APN) including system integrators, consulting firms, and independent software vendors (ISVs). AWS Marketplace, an online software store, helps customers search over 2,300 listings to buy and immediately start using software that runs on AWS.
- **AWS Cloud Security Authorizations and Experience:** AWS offers customers a powerful cloud security capability based on cutting-edge security experience and backed by an extensive repertoire of accreditations and authorizations. In The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014 report, Forrester Research named AWS as the only provider in the Leader category. Forrester stated, "AWS leads the pack. AWS demonstrated not only a broad set of security capabilities in data center security, certifications, and network security, but also excelled in customer satisfaction, security services partnerships, and a large installed base." AWS has achieved two Provisional Authorizations to Operate (P-ATOs) for mission systems

designated by DISA as Cloud Computing Security Requirements Guide (SRG) level 2 (covering all AWS regions in the contiguous United States [CONUS]) and SRG level 4 (covering only the AWS GovCloud (US) Region).

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

Business Benefits of AWS Cloud Services

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

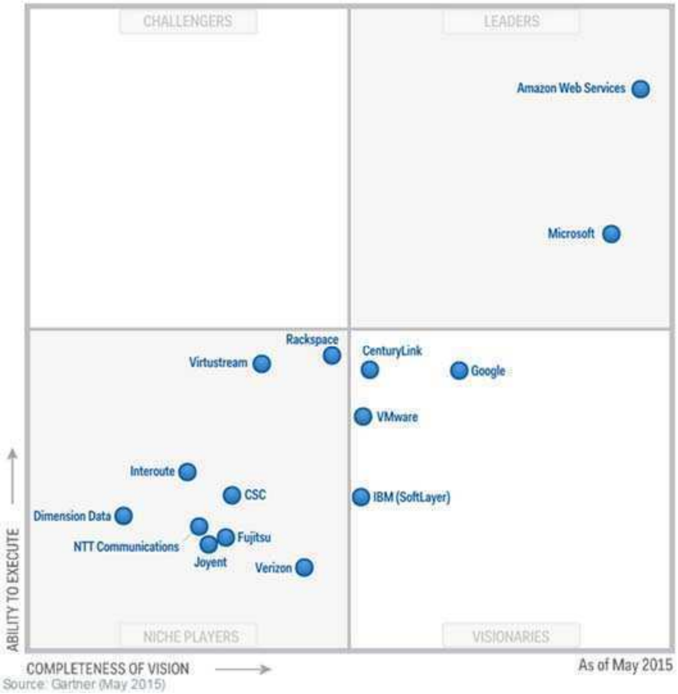
- **Almost Zero Upfront Infrastructure Investment**: If a customer wants to build a large-scale system, it may cost a fortune to invest in real estate, physical security, hardware (racks, servers, routers, backup power supplies), hardware management (power management, cooling), and operations personnel. Because of the high upfront costs, the project would typically require several rounds of management approvals before the project could even get started. With AWS's utility-style cloud computing, there is no fixed cost or startup cost.
- **Just-In-Time Infrastructure**: In the past, if an application became popular and a business' systems or infrastructure did not scale, it became a victim of its own success. Conversely, if a developer invested heavily and did not get popular, it became a victim of failure. By deploying applications in the AWS cloud with just-in-time self-provisioning, customers do not have to worry about pre-procuring capacity for large-scale systems. AWS's cloud increases agility, lowers risk, and lowers operational cost, because customers can scale cloud resources as they grow and only pay for what they use.
- **More Efficient Resource Utilization**: System administrators usually worry about procuring hardware (when they run out of capacity) and higher infrastructure utilization (when they have excess and idle capacity). With AWS, they can manage resources more effectively and efficiently by having the applications request and relinquish resources on-demand.
- **Usage-Based Costing**: With utility-style pricing, AWS customers are billed only for the infrastructure that has been used. AWS customers do not pay for allocated but unused infrastructure. This adds a new dimension to cost savings, allowing customers to see immediate cost savings when they deploy an optimization patch to update their cloud application. For example, if a caching layer can reduce data requests by 70%, the savings begin to accrue immediately. Moreover, if customers build platforms on the cloud, they can pass on the same flexible, variable usage-based cost structure to their own customers.
- **Reduced Time to Market**: Parallelization is the one of the great ways to speed up processing. If one compute-intensive or data-intensive job that can be run in parallel takes 500 hours to process on one machine, with cloud architectures, it would be possible to spawn and launch 500

instances and process the same job in 1 hour. Having available an elastic infrastructure provides the application with the ability to exploit parallelization in a cost-effective manner reducing time to market.

Technical Benefits of AWS Cloud Services

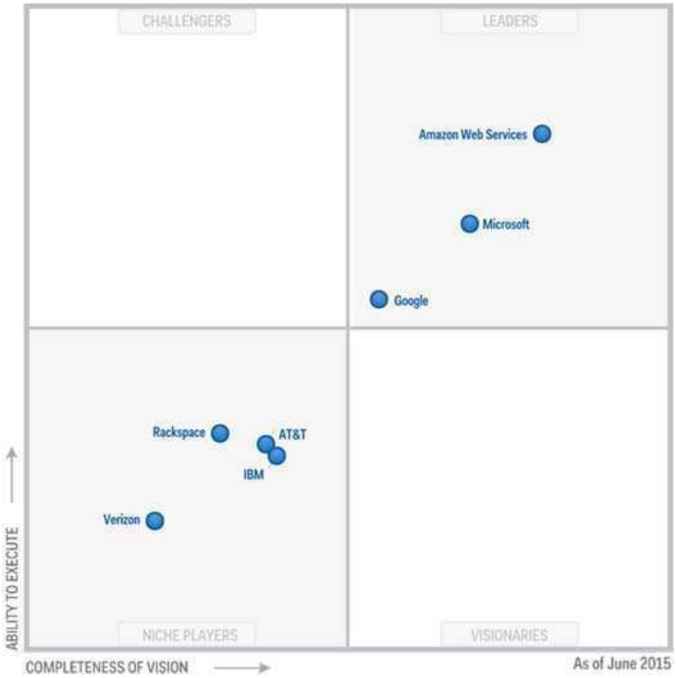
- **Automation – "Scriptable Infrastructure"**: AWS customers can create repeatable build and deployment systems by leveraging programmable (API-driven) infrastructure.
- **Auto Scaling**: AWS customers can scale their applications up and down to match unexpected demand without any human intervention. Auto Scaling encourages automation and drives more efficiency.
- **Proactive Scaling**: Customers can scale applications up and down to meet anticipated demand with proper planning of traffic patterns so that costs remain low while scaling.
- **More Efficient Development Lifecycle**: Production systems may be easily cloned for use as development and test environments. Staging environments may be easily promoted to production.
- **Improved Testability**: Never run out of hardware for testing. Inject and automate testing at every stage during the development process. AWS customers can spin up an "instant test lab" with pre-configured environments only for the duration of testing phase.
- **Disaster Recovery and Business Continuity**: The cloud provides a lower cost option for maintaining a fleet of disaster recovery servers and data storage. With the cloud, customers can take advantage of geo-distribution and replicate the environment in other locations within minutes.
- **Overflow Traffic to the Cloud**: With a few clicks and effective load balancing tactics, customers can create a complete overflow-proof application by routing excess traffic to the cloud.

Analyst Reports: Gartner, Inc., a leading information technology research company, reported in its 2015 Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide report that "AWS is a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market. It has the richest array of IaaS features and PaaS-like capabilities. It continues to rapidly expand its service offerings and offer higher-level solutions." The Gartner Magic Quadrant for May 2015 (**Figure 4**) depicts AWS in the Leaders Quadrant.



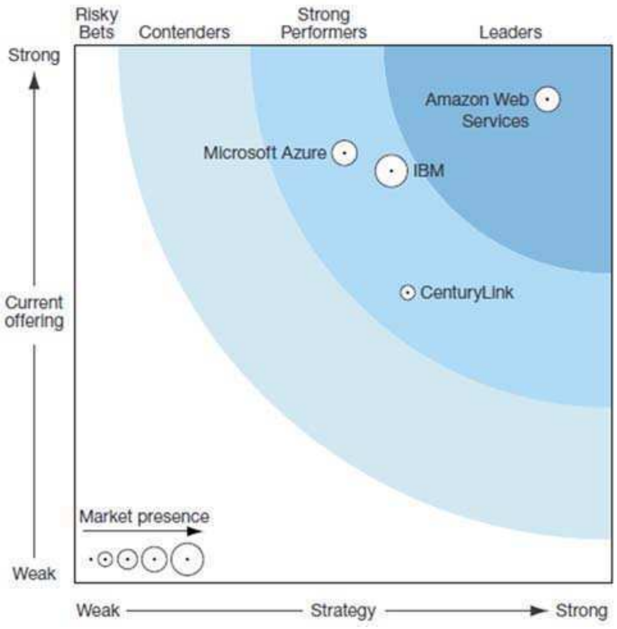
2015 Gartner Magic Quadrant for Cloud Infrastructure as a Service

Additionally, Gartner positions AWS in the Leaders Quadrant of the new Magic Quadrant for Public Cloud Storage Services . Gartner defines leaders as offering innovative storage offerings built on a hardened platform, with global data centers and established credibility as a business.



2015 Gartner Magic Quadrant for Public Cloud Storage Services

The Forrester Wave: Public Cloud Platform Service Providers' Security, Q4 2014 report evaluated four of the leading public clouds along 15 key security criteria, detailing the findings about how well each vendor fulfilled their criteria and where they stand in relation to each other. Forrester's evaluation states "AWS leads the pack. AWS demonstrated not only a broad set of security capabilities in data center security, certifications, and network security, but also excelled in customer satisfaction, security services partnerships, and a large installed base. AWS led with the size of its development and technical support staff as well."



Forrester Wave™: Public Cloud Service Providers' Security, Q4 '14

More analyst reports can be found at http://aws.amazon.com/resources/analyst-reports/

CA Response:

CA Technologies is a leader in IT Management Solutions in the industry. CA has be steadily moving its premier on premise management solutions to the cloud. CA Clarity Project and Portfolio Management (PPM) is one of the leading solutions used by State governments today.

Microsoft Response:

Supported by a winning combination of SHI's Licensing Team and Professional Services, SHI offers the following servers to compliment Microsoft Azure consumption:

- Azure Jumpstart (Onboarding)
- Cloud Assessment & Migration
- Design Planning
- Virtual Network Connectivity
- Virtual Machine Configuration/Migrations
- Cloud Service Architecture
- Azure Storage/StorSimple Migrations
- Azure Website Migrations & HA Architecture

- Azure Application Services
- Azure Active Directory
- Identity Management (SSO, MFA)

6.4.2

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

SHI Response:

SHI is ISO9000 certified. Based on the solutions we provide, we currently do not use SAS 70. As we add partners to support this contract we will review this requirement with them and provide updates to NASPO.

AWS Response:

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

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

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

CA Response:

CA SaaS environment is compliant with SSAE16 for services where infrastructure and application are managed and maintained by CA; certifications can be found here: http://www.ca.com/us/lpg/saas-summary-audit-report.aspx . CA Agile Management currently does not hold SSAE16 certification. For SaaS offerings where infrastructure is managed by a third party, provider's SSAE16 reports are available upon request.

Microsoft Response:

Please see Microsoft Azure CCM Document for complete details.

Azure meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1 and SOC 2. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

- **FedRAMP.** Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program that provides a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies and thereby saves the taxpayer and individual organizations the time and cost of conducting their own independent reviews.
- **FERPA.** The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to use and disclosure restrictions imposed by FERPA.
- **FIPS 140-2.** Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.
- **Comprehensive, independently verified compliance.** Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.
- **CDSA.** The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.
- **CJIS.** Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhere to the same requirements that law enforcement and public safety entities must meet.
- **CSA CCM.** The Cloud Security Alliance (CSA) is a nonprofit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

- **EU Model Clauses.** Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world.
- **FDA 21 CFR Part 11.** The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.
- **HIPAA.** The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.
- **IRAP.** Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.
- **ISO/IEC 27018.** Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
- **ISO/IEC 27001/27002:2013.** Azure complies with this standard, which defines the security controls required of an information security management system.
- **MLPS.** Multi-Level Protection Scheme (MLPS) is based on the Chinese state standard issued by the Ministry of Public Security. Azure operated by 21Vianet adheres to this standard, which provides assurance for both the management and technical security of cloud systems.
- **MTCS.** Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard covering areas such as data security, confidentiality, business impact, and operational transparency, developed under the Singapore Information Technology Standards Committee.
- **PCI DSS.** Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.
- **SOC 1 and SOC 2.** Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.
- **TCS CCCPPF.** Azure operated by 21Vianet is among the first cloud providers in China to pass the Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF).
- **UK G-Cloud.** The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor.

6.5 Billing And Pricing Practices

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

6.5.1

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

SHI Response:

Many of the solutions that will be procured through this contract will be usage based, meaning, NASPO Entities will be billed only for what they use in a specific month or quarter. Each partner has a different strategy for usage based billing. SHI works to normalize these practices to our customers. In cases such as these SHI will work upfront with both the customer and the partner to make sure that the billing practices meet the customers' needs. Regardless of the solution, we will supply a transparent usage report to the customer so they can easily determine the accuracy.   If awarded, SHI will adhere to the contracted discount structure agreed to and make this transparent on our quotes and invoices to the customer.

If at any time there is a question or concern with an invoice, a Participating State can contact their Account Executive or Inside Sales Representative for assistance.

6.5.2

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

SHI Response:

SHI works closely with each of our customers during the "Address" phase as identified in 6.4.1 to ensure they understand the financial impacts they will incur when moving to the cloud. It is important not only to look at the immediate cost but also to analyze the cost over time so the customer can budget correctly.

Some Cloud solutions will be a one-time fee or a licensing program, while others may use a utility-style pricing model, only paying for the resources consumed. Whatever the model, SHI has a team dedicated to support customers.

While some Participating Entities may have a clear understanding of the solution they want to use others are just beginning to explore their options. SHI helps to educate our customers on the importance of analyzing current infrastructure before migrating to the cloud. The dedicated account teams will have pre-sales, vendor neutral discussions covering topics such as:

- The people, processes, and technology that will be affected by a move to the cloud
- Understanding the risks and create compliance plans
- Identity and access management
- Security as a foundational component of cloud deployment
- Categorizing Data and determining what data is a good candidate for migration
- Analyzing workloads

When these critical issues are addressed before customers choose and deploy cloud solutions NASPO Participating Entities will realize significant cost savings.

Your SHI team will work with you every day to help analyze your spending, your current and future projects, and buying alternatives. The savings that States realize when working with SHI to plan and negotiate their Cloud Solutions direction can be in the thousands, hundreds of thousands, or even millions of dollars.

6.5.3

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

SHI Response:

While SHI does not manufacturer or offer our own products and solutions, we do work with the top partners in the industry. The products that we are responding with today all comply with NIST. As we work to add partners and solutions we will ensure that they NIST compliant.

AWS Response:

AWS's industry-leading security strength benefits you in many ways, one of which is by using a platform that is audited extensively by independent third-party assessors. At times, these audits confirm we can meet new requirements, even as they are issued, and this is the case for the National Institute of Standards and Technology (NIST) guidelines 800-171, which were released in June 2015. This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on nonfederal systems.

AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which we have already been audited under our FedRAMP program. The FedRAMP Moderate security control baseline is ***more*** rigorous than the recommended requirements established in Chapter 3 of 800-171 and includes a significant number of security controls above and beyond those required of FISMA Moderate systems that protect CUI data. A detailed mapping is available in the NIST Special Publication 800-171, starting on page D2 (which is page 37 in the PDF).

Microsoft Response:

Both Azure and the underlying Microsoft Cloud and Infrastructure Operations (MCIO) physical environments employ security frameworks that span multiple standards, including the ISO 27000 family of standards, NIST 800, and others. Please see Microsoft Azure CCM document for additional information.

6.6 Scope And Variety Of Cloud Solutions

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

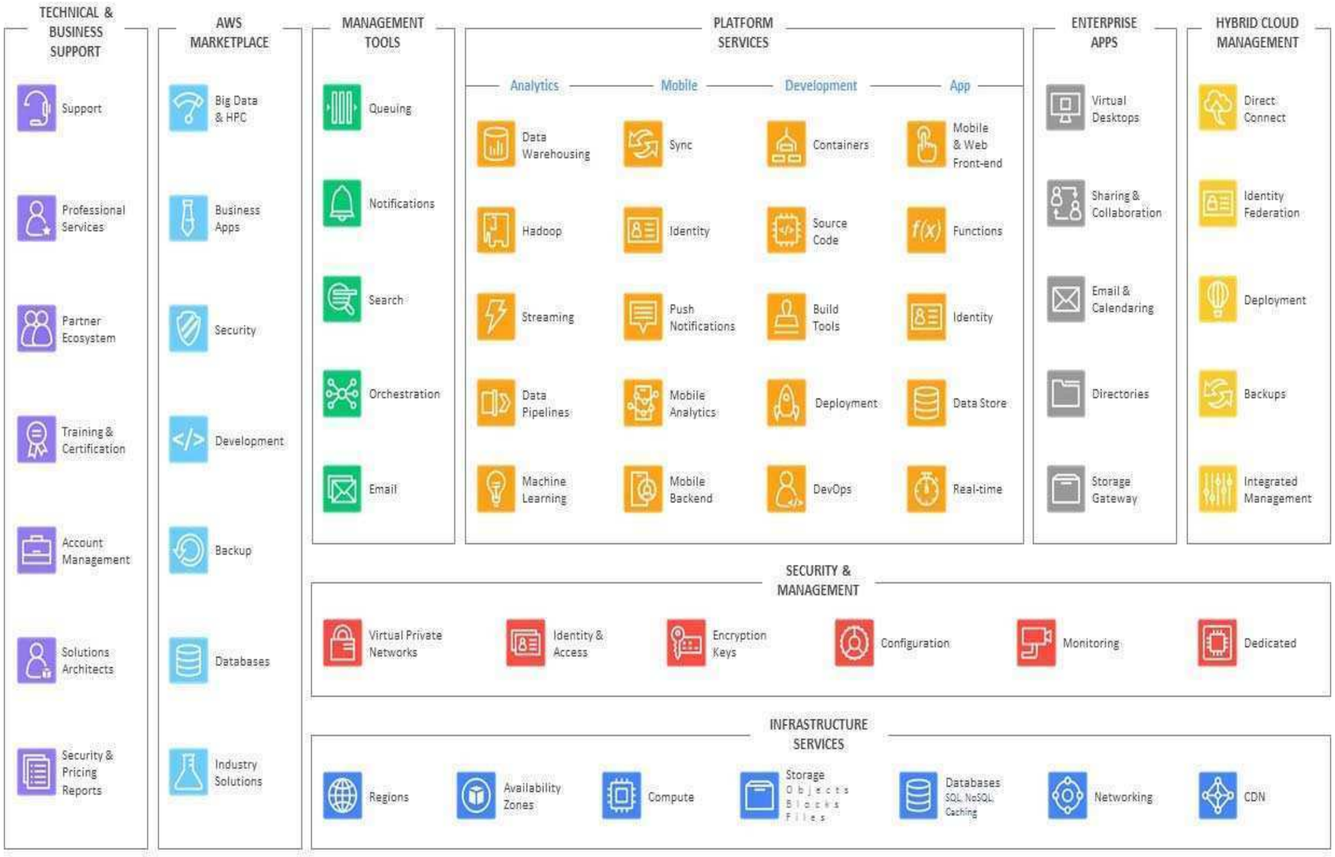
SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations.

AWS Response:

AWS offers a Public Cloud as the customer decides how, when, and how they are using. AWS has additional tools and features.



CA Response:

CA Technologies provides SaaS solutions that help agencies from planning to development to software development to enabling online business with security. CA Technologies help jump start the IT process so that agencies can become more agile and manage their IT operations with more efficiency and lower cost. CA Technologies offers a portfolio of five different SaaS Applications to enable agencies to be thrive in the application economy.

CA Project Portfolio Management (CA PPM)

CA PPM represents a single platform that enables you to manage your entire innovation lifecycle and make more informed strategic investments. CA PPM helps you track and prioritize market and customer requirements and make better decisions on how to invest limited resources, so you can optimize your enterprise, IT, service and product portfolio, delivering initiatives on time and on budget.

CA Agile Central

Agile is a mindset that changes how you deliver value to your customers—one that transforms market strategy into marketable innovation. When you're agile, the right people will always get access to the right information, faster than ever before. You'll remove the barriers that separate your teams. CA Agile Central provides the tools and training to make your teams more agile.

CA Application Synthetic Monitoring (CA ASM)

CA Application Synthetic Monitoring in unique application for Website Performance Monitoring.

CA App Synthetic Monitor has the ability to provide true end user experience and performance monitoring by conducting checks from an external sites to replicate an actual, real-time user experience and provides your business with hard data about your website's performance and availability.

CA App Synthetic Monitor can be setup up immediately to start reporting with analysis and alerting, using pre-built scripts. CA App Synthetic Monitor also has a powerful API that integrates seamlessly with your enterprise APM solution.

CA Application Performance Monitoring (CA APIM)

APIs are the building blocks of digital transformation.

States have the unique opportunity to open of the troves of data and transform society by providing citizens access to high-quality digital information right on their mobile devices, when and where they want it. CA API Management provides the tools to both accelerate and secure this digital transformation.

CA Mobile Apps Analytics (CA MAA)

With more mobile devices than people, the secret to a successful mobile app? A great user experience.

CA Mobile App Analytics provides developers and tests with the tools to get your app firing on all cylinders. It provides the ability to monitor, analyze and fix your app on the fly. CA Mobile App Analytics stimulates collaboration between business analysts, developers, operations and support in order to accelerate mobile app delivery and improve end-user experience. By emulating and fixing problems before you go live, you dramatically improve your customer experience.

Microsoft Response:

Azure Active Directory B2C

Azure Active Directory, the cloud service with the proven ability to handle billions of authentications per day, extends its capabilities to manage consumer identities with a new service: Azure Active Directory B2C, now in public preview. Azure Active Directory B2C is a comprehensive, identity management solution for your consumer-facing applications that can be easily integrated to any platform, and accessible from any device. The service will be free during the public preview period.

Azure Active Directory

Azure Active Directory provides identity management and access control for your cloud applications. To simply user access to cloud applications, you can synchronize on-premises identities, and enable single sign-on. Azure Active Directory comes in 3 editions: Free, Basic, and Premium.

Azure Active Directory Domain Services

Azure Active Directory Domain Services provide scalable, high-performance, managed domain services such as domain-join, LDAP, Kerberos, Windows Integrated Authentication and Group Policy support. With the click of a button, administrators can enable managed domain services for virtual machines and directory-aware applications deployed in Azure Infrastructure Services. Built on the same underlying technology as Windows Server Active Directory, Azure Active Directory Domain Services provide an easy way to migrate traditional on-premises applications to the cloud.

API Management

Azure API Management lets you publish APIs to developers, partners, and employees securely and at scale.

Application Gateway

Azure Application Gateway is an Azure-managed layer-7 solution providing HTTP load balancing, SSL termination, and session-based cookie affinity to Internet-facing or internal web applications.

Visual Studio Application Insights

Visual Studio Application Insights (in preview) is an all-in-one telemetry solution that can help you detect issues, triage impact and solve problems in your web apps and services. It provides deep diagnostics and real-time insights while being a seamless part of your ALM processes through Visual Studio, Visual Studio Team Services, and Azure Diagnostics integrations. It supports ASP.NET, J2EE and most of the popular web technologies for web apps on Azure or on your own servers.

App Service

Azure App Service lets you create apps faster with a one-of-a kind cloud service to quickly and easily create enterprise-ready web and mobile apps for any platform or device and deploy them on a scalable and reliable cloud infrastructure.

Automation

Azure Automation lets you create, deploy, monitor, and maintain resources in your Azure environment automatically by using a highly scalable and reliable workflow execution engine.

Backup

On your corporate laptops, Azure Backup protects Windows client data and shared files and folders. In your datacenter, integrated with System Center Data Protection Manager (DPM), Backup protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications.

Batch

Azure Batch makes it easy to run large-scale parallel and high-performance computing (HPC) workloads in Azure. Use Batch to scale out parallel workloads, manage the execution of tasks in a queue, and cloud-enable applications to offload compute jobs to the cloud.

BizTalk Services

Azure BizTalk Services is a powerful and extensible cloud-based integration service. It provides B2B and EAI capabilities for delivering cloud and hybrid integration solutions.

CDN

Azure Content Delivery Network lets you deliver high-bandwidth content to users around the world with low latency and high availability via a robust network of global data centers.

Cloud Services

Azure Cloud Services removes the need to manage server infrastructure. With web and worker roles, it lets you quickly build, deploy, and manage modern applications.

Azure Container Service

Azure Container Service is a container hosting environment optimized for Azure that lets you deploy, scale, and orchestrate container-based applications using Docker Swarm and Apache Mesos—popular, open source tools you’re already familiar with.

Data Catalog

Azure Data Catalog is a fully managed service that serves as a system of registration and system of discovery for enterprise data sources. It lets users—from analysts to data scientists to developers—register, discover, understand, and consume data sources. Use crowdsourced annotations and metadata to capture tribal knowledge within your organization, shine light on hidden data, and get more value from your enterprise data sources.

Data Factory

Azure Data Factory is a managed service that lets you produce trusted information from raw data in cloud or on-premises sources. Easily create, orchestrate, and schedule highly-available, fault-tolerant work flows of data movement and transformation activities. Monitor service health and all of your data pipelines at a glance with a rich visual experience offered through the Azure portal.

Data Lake Analytics

The Data Lake analytics service is a new distributed analytics service built on Apache YARN that dynamically scales so you can focus on your business goals, not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by simply setting the dial for how much power you need. You only pay for your job when it is running making it cost-effective. The analytics service supports Azure Active Directory letting you simply manage access and roles, integrated with your on-premises identity system. It also includes U-SQL, a language that unifies the benefits of SQL with the expressive power of user code. U-SQL's scalable distributed runtime enables you to efficiently analyze data in the store and across SQL Servers in Azure, Azure SQL Database and Azure SQL Data Warehouse.

Data Lake Store

The Data Lake store provides a single repository where you can capture data of any size type and speed simply without forcing changes to your application as the data scales. In the store, data can be shared for collaboration with enterprise-grade security. It is also designed for high-performance processing and analytics from HDFS applications (ie. Azure HDInsight, Data Lake analytics service, Hortonworks, Cloudera, MapR) and tools, including support for low latency workloads. For example, data can be ingested in real-time from sensors and devices for IoT solutions, or from online shopping websites into the store without the restriction of fixed limits on account or file size unlike current offerings in the market.

Azure DevTest Labs

Azure DevTest Labs makes it easy to quickly create environments to deploy and test applications. Use reusable templates and artifacts to build Windows and Linux environments while minimalizing waste and controlling costs.

Azure DNS

Azure DNS lets you host your DNS domains alongside your Azure apps and manage DNS records by using your existing Azure subscription. Microsoft's global network of name servers has the reach, scale, and redundancy to ensure ultra-fast DNS responses and ultra-high availability for your domains. With Azure DNS, you can be sure your DNS will always be fast and available.

DocumentDB

Azure DocumentDB is a fully-managed NoSQL document database service that offers querying and transaction-processing over schema-free data, predictable and reliable performance, and rapid development.

Event Hubs

Azure Event Hubs enables elastic-scale telemetry and event ingestion with durable buffering and sub-second end-to-end latency for millions of devices and events.

ExpressRoute

Azure ExpressRoute lets you create private connections between Azure datacenters and infrastructure that's on your premises or in a colocation environment.

HDInsight

Azure HDInsight is a Hadoop-based service that brings an Apache Hadoop solution to the cloud. Gain the full value of big data with a cloud-based data platform that manages data of any type and size.

Azure IoT Hub

Jumpstart your Internet of Things project with Microsoft Azure IoT Hub. Connect, monitor, and control millions of IoT assets running on a broad set of operating systems and protocols. Establish reliable, bi-directional communication with these assets, even if they're intermittently connected, and analyze—and act on—incoming telemetry data. Enhance the security of your IoT solutions by using per-device authentication to communicate with devices that have the appropriate credentials. Revoke access rights to specific devices to maintain the integrity of your system.

Key Vault

Azure Key Vault offers an easy, cost-effective way to safeguard keys and other secrets in the cloud by using hardware security modules (HSMs). Protect cryptographic keys and small secrets like passwords with keys stored in HSMs. For added assurance, import or generate your keys in HSMs that are certified to FIPS 140-2 level 2 and Common Criteria EAL4+ standards, so that your keys stay within the HSM boundary. Key Vault is designed so that Microsoft does not see or extract your keys. Create new keys for Dev-Test in minutes and migrate seamlessly to production keys managed by security operations. Key Vault scales to meet the demands of your cloud applications without the hassle required to provision, deploy, and manage HSMs and key management software.

Load Balancer

Azure Load Balancer distributes Internet and private network traffic among healthy service instances in cloud services or virtual machines. It lets you achieve greater reliability and seamlessly add more capacity to your applications.

Machine Learning

Azure Machine Learning lets you easily design, test, operationalize, and manage predictive analytics solutions in the cloud.

Managed Cache Service

Azure Managed Cache Service is a distributed, in-memory, scalable solution that lets you build highly scalable and responsive applications by providing super-fast access to data.

Media Services

Azure Media Services offers cloud-based media solutions, including ingest, encoding, format conversion, content protection, and both on-demand and live-streaming capabilities.

Mobile Engagement

Azure Mobile Engagement lets you maximize mobile app usage and revenue. It's an SaaS-delivered, data-driven user-engagement platform that enables real-time, fine-grained user segmentation, app user analytics, and contextually-aware smart-push notifications and in-app messaging across all connected devices. It closes the marketing loop for app developers and marketers, letting them get directly in touch with all of their customers in a personal, contextually-aware, and non-intrusive way, and at the right time.

Mobile Services

Azure Mobile Services is a scalable cloud backend for building Windows Store, Windows Phone, Apple iOS, Android, and HTML/JavaScript applications. Store data in the cloud, authenticate users, and send push notifications to your application within minutes.

Multi-Factor Authentication

Azure Multi-Factor Authentication helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. Follow organizational security and compliance standards while also addressing user demand for convenient access.

Notification Hubs

Azure Notification Hubs is a highly scalable, cross-platform push notification infrastructure that lets you either broadcast push notifications to millions of users at once or tailor notifications to individual users.

Operational Insights

Azure Operational Insights lets you collect, correlate and visualize all your machine data, such as event logs, network logs, performance data, and much more, from both your on-premises and cloud assets.

Redis Cache

Azure Redis Cache—based on the popular open source Redis cache—gives you access to a secure, dedicated cache for your Azure applications.

RemoteApp

Azure RemoteApp helps employees stay productive anywhere, on a variety of devices—Windows, Mac OS X, iOS, or Android.

Scheduler

Azure Scheduler lets you invoke actions that call HTTP/S endpoints or post messages to a storage queue on any schedule. Create jobs that reliably call services either inside or outside of Azure and run those jobs right away, on a regular or irregular schedule, or at a future date.

Search

Azure Search is a fully-managed service for adding sophisticated search capabilities to web and mobile applications without the typical complexities of full-text search.

Security Center

Azure Security Center helps you prevent, detect, and respond to threats with increased visibility and control over the security of all of your Azure resources. It provides a central view of security across your subscriptions and lets you set policies and monitor security configurations. Policy-driven recommendations guide resource owners through the process of implementing security controls and enable the rapid deployment of integrated Microsoft and partner solutions. Using Microsoft global threat intelligence, security-related events from across your Azure deployments are automatically collected and analyzed to identify actual threats and reduce false alarms. The resulting alerts offer insights into the attack and suggest ways to remediate issues.

Service Bus

Azure Service Bus is a messaging infrastructure that sits between applications allowing them to exchange messages for improved scale and resiliency.

Service Fabric

Service Fabric is a microservices platform used to build scalable, reliable, and easily managed applications for the cloud. Addressing the significant challenges in developing and managing cloud applications, Service Fabric allows developers and administrators to avoid solving complex infrastructure problems and focus instead on implementing mission-critical, demanding workloads.

Site Recovery

Azure Site Recovery helps you protect important applications by coordinating the replication and recovery of private clouds for simple, cost-effective disaster recovery.

SQL Database

Azure SQL Database is a relational database service that lets you rapidly create, extend, and scale relational applications into the cloud.

SQL Data Warehouse

Azure SQL Data Warehouse is an elastic data warehouse as a service with enterprise-grade features based on the massively parallel SQL Server processing architecture. It lets you scale data, either on-premises or in our cloud. It's the first cloud data warehouse that can dynamically grow or shrink, so you pay only for the query performance that you need, when you need it, up to petabyte-scale. SQL Data Warehouse lets you use your existing Transact-SQL (T-SQL) skills to integrate queries across structured and unstructured data. SQL Data Warehouse integrates with our data platform tools, including Azure HDInsight, Machine Learning, and Data Factory and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud. With SQL Data Warehouse, you choose where to keep your data, either in the cloud or on-premises, based on your performance, security, and scale requirements.

SQL Server Stretch Database

With SQL Server Stretch Database, you can dynamically stretch warm and cold transactional data from Microsoft SQL Server to Azure. Unlike typical cold data storage, your data is always at hand. Stretch Database lets you provide longer data retention times than typical enterprise storage without breaking the bank. Depending on how often you'll access the data, choose the appropriate level of service, then scale up or down as needed. Using Stretch Database doesn't require any application changes. And you can use Stretch Database with new Always Encrypted technology, which helps protect your data at rest and in motion—extending data in a more secured manner for greater peace of mind.

Storage

Azure Storage offers non-relational data storage including Blob Storage, Table Storage, Queue Storage, and Files.

StorSimple

Azure StorSimple is a unique hybrid cloud storage solution for primary storage, archiving, and disaster recovery. StorSimple optimizes total storage costs and data protection. Note that the StorSimple 8000 Series is licensed separately from Azure services.

Stream Analytics

Azure Stream Analytics is an event-processing engine that helps you gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. It's integrated out of the box with Event Hubs, and the combined solution can both ingest millions of events and do analytics to help you better understand patterns, power a dashboard, detect anomalies, or kick off an action while data is being streamed in real time.

Traffic Manager

Azure Traffic Manager lets you route incoming traffic across multiple hosted Azure services, whether they're running in the same datacenter or in different datacenters around the world.

Virtual Machines

Azure Virtual Machines lets you deploy a Windows Server or Linux image in the cloud. You can select images from a marketplace or use your own customized images.

Virtual Network

Azure Virtual Network lets you create private networks in the cloud with full control over IP addresses, DNS servers, security rules, and traffic flows. Securely connect a virtual network to on-premises networks by using a VPN tunnel, or connect privately by using the ExpressRoute service.

Visual Studio Team Services

Visual Studio Team Services is a cloud-based application lifecycle management (ALM) solution for everything from hosted-code repositories and issue-tracking to load-testing and automated builds. It's accessible from nearly anywhere, and you can create an account for free. Visual Studio Team Services is licensed separately from Azure services.

VPN Gateway

Azure VPN Gateway lets you establish secure, cross-premises connections between your virtual network within Azure and on-premises IT infrastructure.

6.7 Best Practices

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

SHI Response:

SHI doesn’t develop cloud solutions but we are partnering with several cloud partners to respond to this RFP and will continue to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise. As we add partners, we will ensure that we can provide their best practices regarding policies and procedures as requested by NASPO.

AWS Response:

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

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

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

Built-In Security Features

Not only are applications and data protected by highly secure facilities and infrastructure, they are also protected by extensive network and security monitoring systems. AWS and its partners offer over 700 tools and features to help customers meet their security objectives concerning visibility, auditability, controllability, and agility. These tools and features provide basic but important security measures such as Distributed Denial of Service (DDoS) protection and password brute-force detection on AWS accounts. AWS-provided security features include:

- **Secure Access** – Customer access points, also called Application Programming Interface (API) endpoints, allow secure HTTP access (HTTPS) so that customers can establish secure communication sessions with their AWS cloud services using Secure Socket Layer (SSL)/Transport Layer Security (TSL).
- **Built-In Firewalls** – Customers can control how accessible their instances are by configuring built-in firewall rules—from totally public to completely private or somewhere in between. And

when instances reside within an Amazon Virtual Private Cloud (Amazon VPC) subnet, customers can control egress as well as ingress.

- **Unique Users** – The AWS Identity and Access Management (IAM) tool allows AWS customers to control the level of access their own users have to AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
- **Multi-Factor Authentication (MFA)** – AWS provides built-in support for MFA for use with AWS accounts as well as individual AWS IAM user accounts.
- **Private Subnets** – The Amazon VPC service allows customers to add another layer of network security to instances by creating private subnets and even adding an Internet Protocol Security (IPsec) Virtual Private Network (VPN) tunnel between a home network and Amazon VPC.
- **Encrypted Data Storage** – Customers can have the data and objects they store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- **Dedicated Connection Option** – The AWS Direct Connect service allows customers to establish a dedicated network connection from their premises to AWS. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS cloud.
- **Isolated GovCloud** – For customers who require additional measures in order to comply with US International Traffic in Arms Regulations (ITAR), AWS offers an entirely separate region called AWS GovCloud (US). This isolated region provides an environment where customers can run ITAR-compliant applications and provides special endpoints that utilize only Federal Information Processing Standard (FIPS) 140-2 encryption.
- **Dedicated, Hardware-Based Crypto Key Storage Option** – For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
- **Centralized Key Management** – For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.
- **Perfect Forward Secrecy** – For even greater communication privacy, several AWS cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.

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

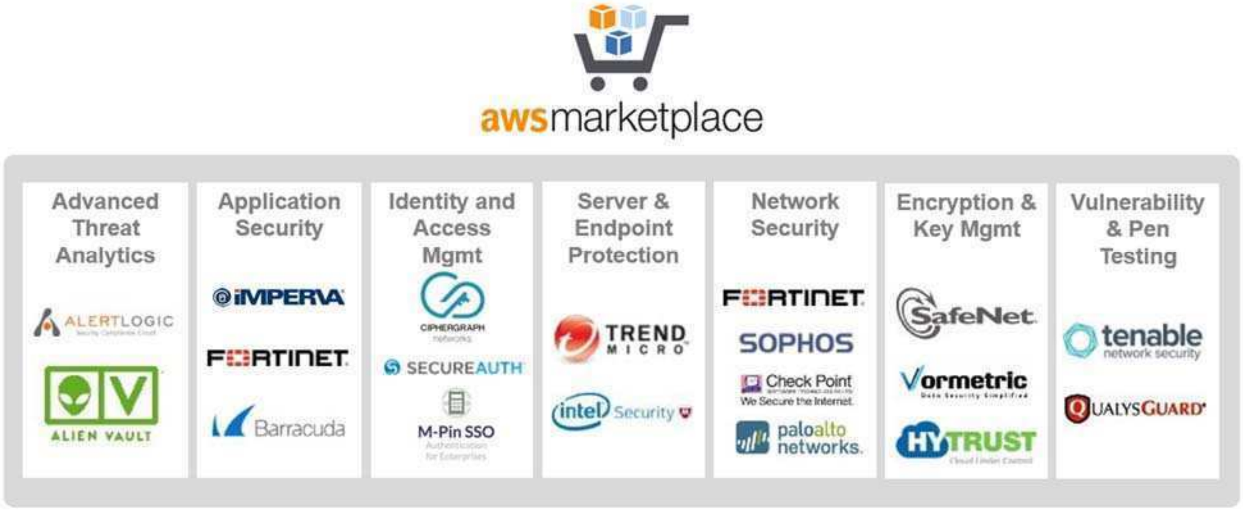
- **AWS Trusted Advisor** – Provided automatically when AWS customers sign up for premium support, the AWS Trusted Advisor service is a convenient way for customers to see where they could use a little more security. It monitors AWS resources and alerts customers to security configuration gaps such as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

- **Amazon CloudWatch** – Amazon CloudWatch enables customers to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by a customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.
- **AWS CloudTrail** – AWS CloudTrail provides logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS cloud service. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.
- **AWS Config** – With the AWS Config service, customers can immediately discover all of their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.

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

Third-Party Security Tools

We also offer additional third-party security tools to complement and enhance our customers' operations in the AWS cloud. AWS Partner Network (APN) partners offer hundreds of familiar and industry-leading products that are equivalent to, identical to, or integrate with existing controls in a customer's on-premises environments. Customers can browse and purchase APN partner products on the AWS Marketplace. These products complement existing AWS cloud services to enable customers to deploy a comprehensive security architecture and a more seamless experience across their cloud and on-premises environments. The APN partner security products cover multiple areas of security, including application security, policy management, identity management, security monitoring, vulnerability management, and endpoint protection. Error! Reference source not found. is a snapshot of the APN partners and categories of products available under the security category in the AWS Marketplace.



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

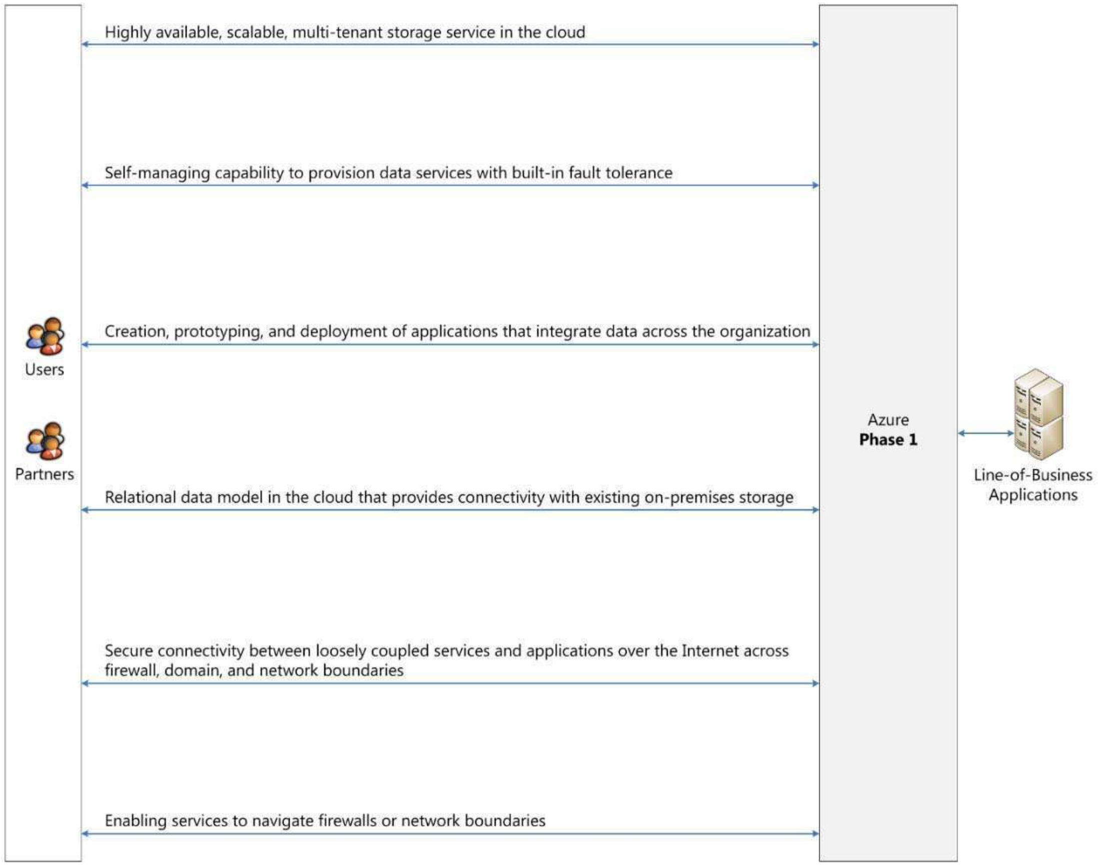
CA Response:

This is addressed throughout all of our policies and procedures. CA SaaS Operations and Delivery runs an Information Security Management Framework (ISMS), which includes security organization, documentation, monitoring, and continuous improvement cycle. The security documentation comprises of CA SaaS Operations information security policies, procedures, guidelines and checklists. ISMS documentation is reviewed along with applicable controls annually. CA offers a variety of SaaS solutions, details for each offering has been provided in Exhibit 1 and 2 of this proposal.

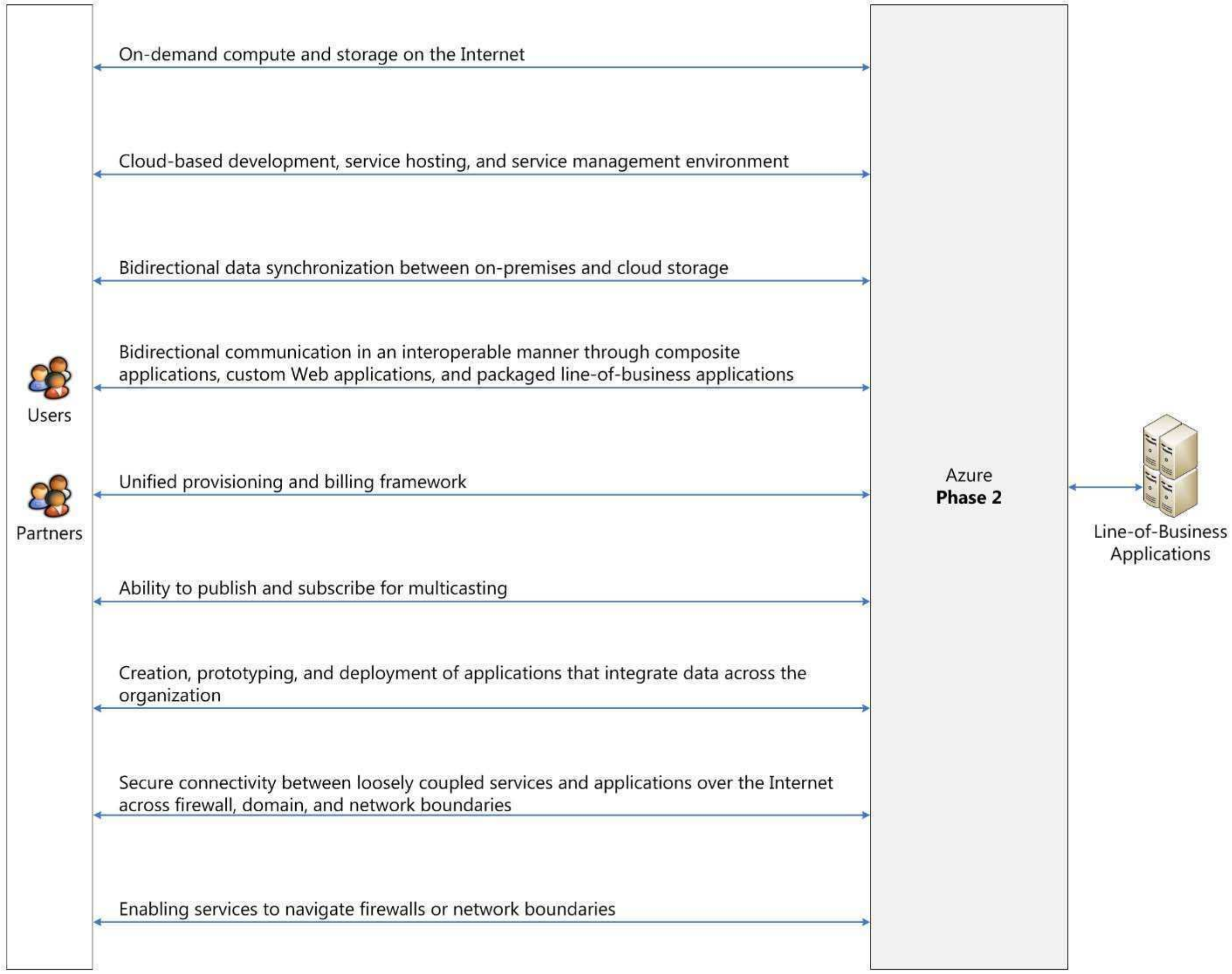
Microsoft Response:

Below are diagrams that illustrate the policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services with Microsoft.

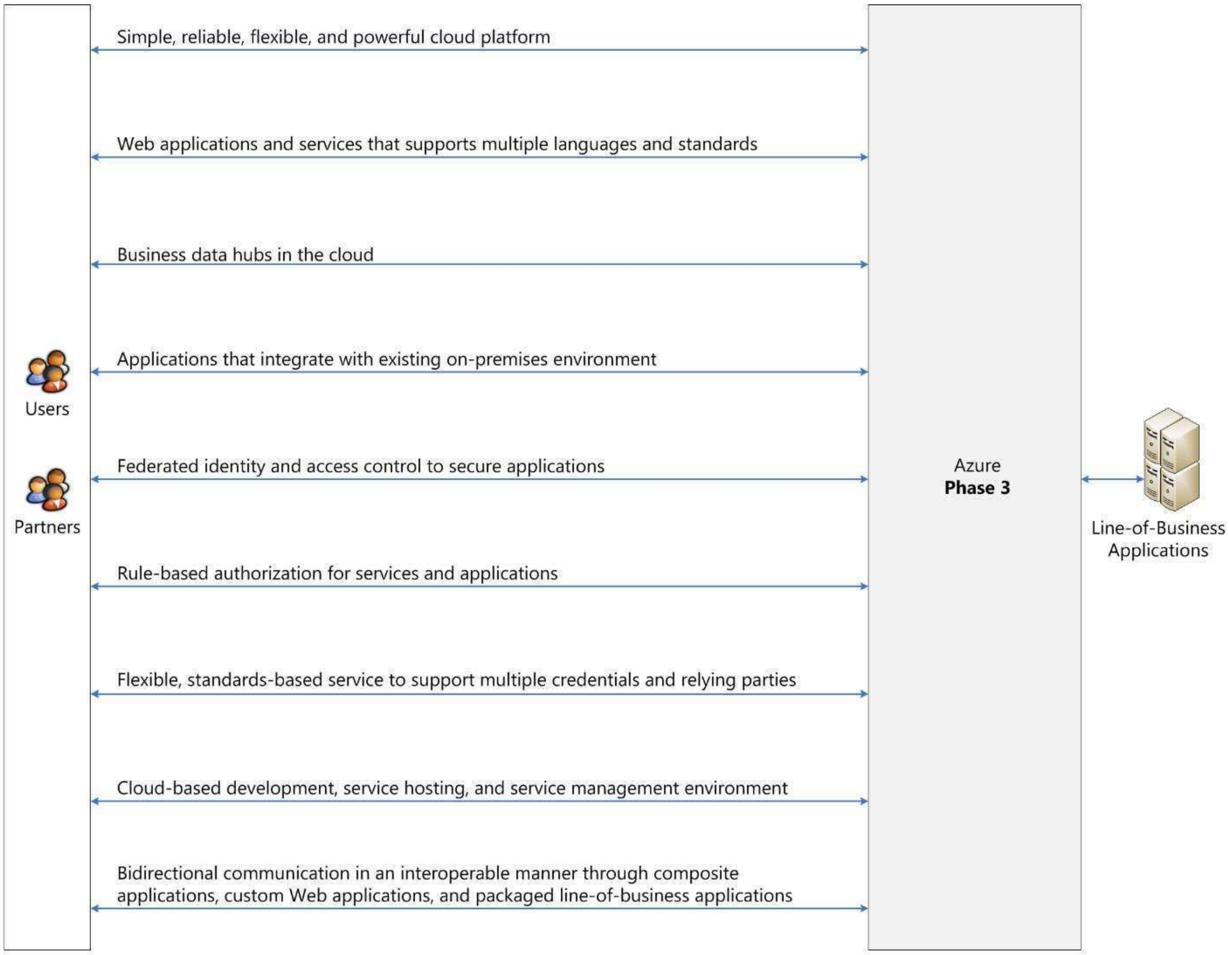
Azure Conceptual Design Phase 1


Highly available, scalable, multi-tenant storage service in the cloud
Self-managing capability to provision data services with built-in fault tolerance
Creation, prototyping, and deployment of applications that integrate data across the organization
Users
Partners
Relational data model in the cloud that provides connectivity with existing on-premises storage
Secure connectivity between loosely coupled services and applications over the Internet across firewall, domain, and network boundaries
Enabling services to navigate firewalls or network boundaries
Azure
Phase 1
Line-of-Business Applications

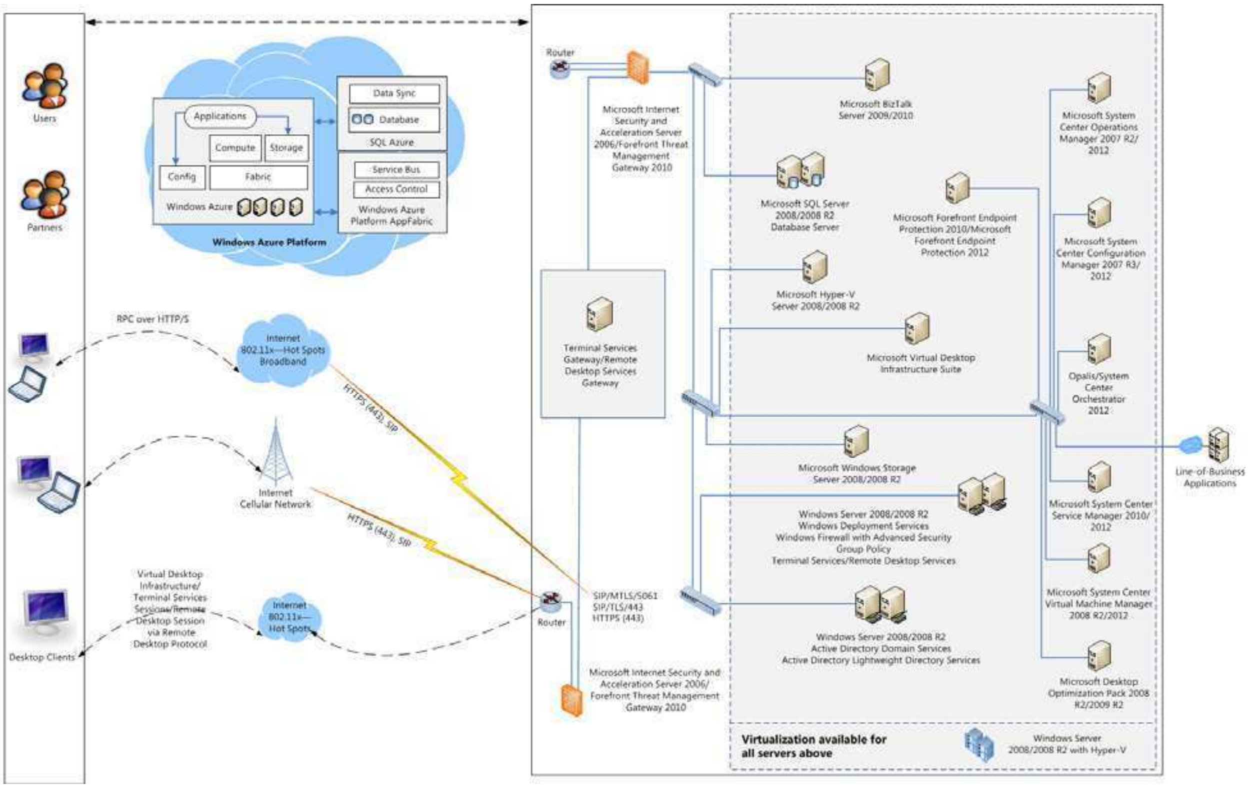
Azure Conceptual Design Phase 2


On-demand compute and storage on the Internet
Cloud-based development, service hosting, and service management environment
Bidirectional data synchronization between on-premises and cloud storage
Bidirectional communication in an interoperable manner through composite applications, custom Web applications, and packaged line-of-business applications
Users
Unified provisioning and billing framework
Partners
Azure
Phase 2
Line-of-Business Applications
Ability to publish and subscribe for multicasting
Creation, prototyping, and deployment of applications that integrate data across the organization
Secure connectivity between loosely coupled services and applications over the Internet across firewall, domain, and network boundaries
Enabling services to navigate firewalls or network boundaries

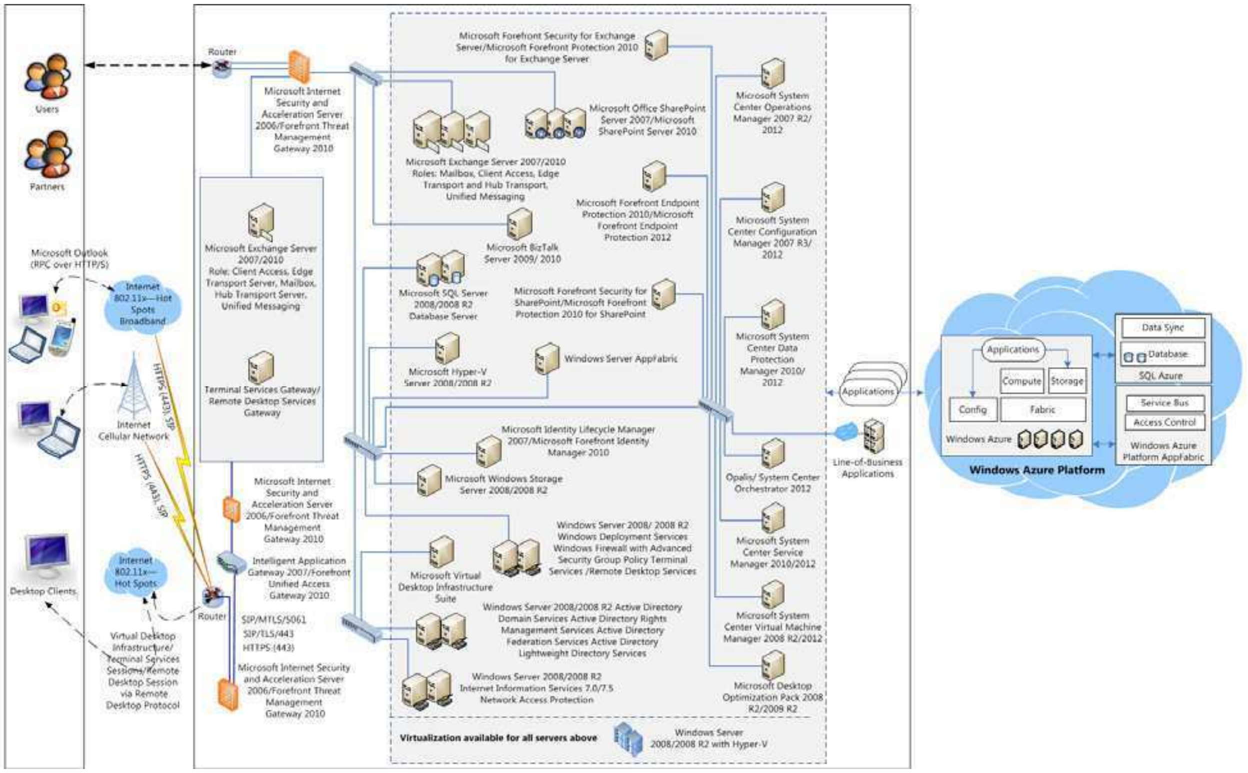
Azure Conceptual Design Phase 3


Simple, reliable, flexible, and powerful cloud platform
Web applications and services that supports multiple languages and standards
Business data hubs in the cloud
Applications that integrate with existing on-premises environment
Users
Federated identity and access control to secure applications
Partners
Azure
Phase 3
Line-of-Business
Applications
Rule-based authorization for services and applications
Flexible, standards-based service to support multiple credentials and relying parties
Cloud-based development, service hosting, and service management environment
Bidirectional communication in an interoperable manner through composite
applications, custom Web applications, and packaged line-of-business applications

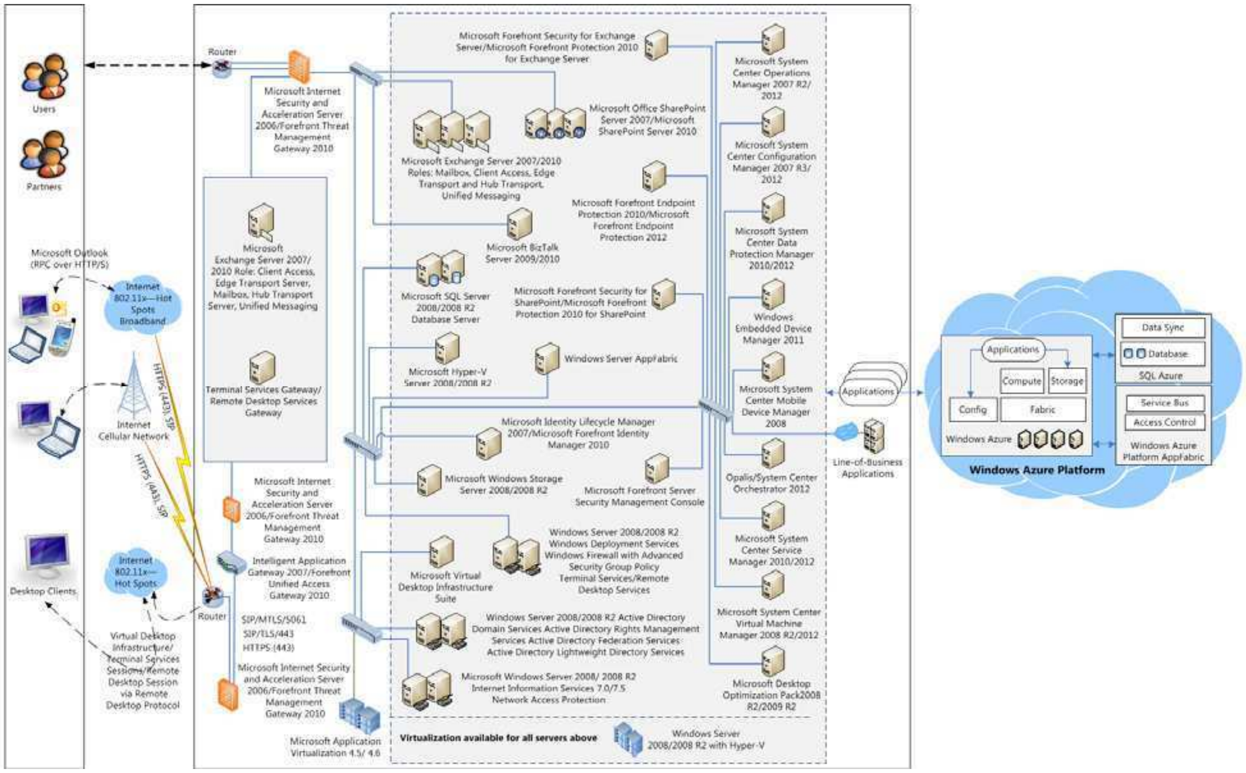
Azure Physical Design Phase 1


Users
Partners
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform
RPC over HTTP/S
Internet 802.11x—Hot Spots Broadband
HTTPS (443), SIP
Internet Cellular Network
HTTPS (443), SIP
Virtual Desktop Infrastructure/ Terminal Services Sessions/Remote Desktop Session via Remote Desktop Protocol
Internet 802.11x—Hot Spots
Desktop Clients
Router
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Terminal Services Gateway/Remote Desktop Services Gateway
SIP/MTLS/5061
SIP/TLS/443
HTTPS (443)
Router
Microsoft Internet Security and Acceleration Server 2006/ Forefront Threat Management Gateway 2010
Microsoft BizTalk Server 2009/2010
Microsoft SQL Server 2008/2008 R2 Database Server
Microsoft Forefront Endpoint Protection 2010/Microsoft Forefront Endpoint Protection 2012
Microsoft Hyper-V Server 2008/2008 R2
Microsoft Virtual Desktop Infrastructure Suite
Microsoft Windows Storage Server 2008/2008 R2
Windows Server 2008/2008 R2
Windows Deployment Services
Windows Firewall with Advanced Security
Group Policy
Terminal Services/Remote Desktop Services
Windows Server 2008/2008 R2
Active Directory Domain Services
Active Directory Lightweight Directory Services
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Opalis/System Center Orchestrator 2012
Line-of-Business Applications
Microsoft System Center Service Manager 2010/ 2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Microsoft Desktop Optimization Pack 2008 R2/2009 R2
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V

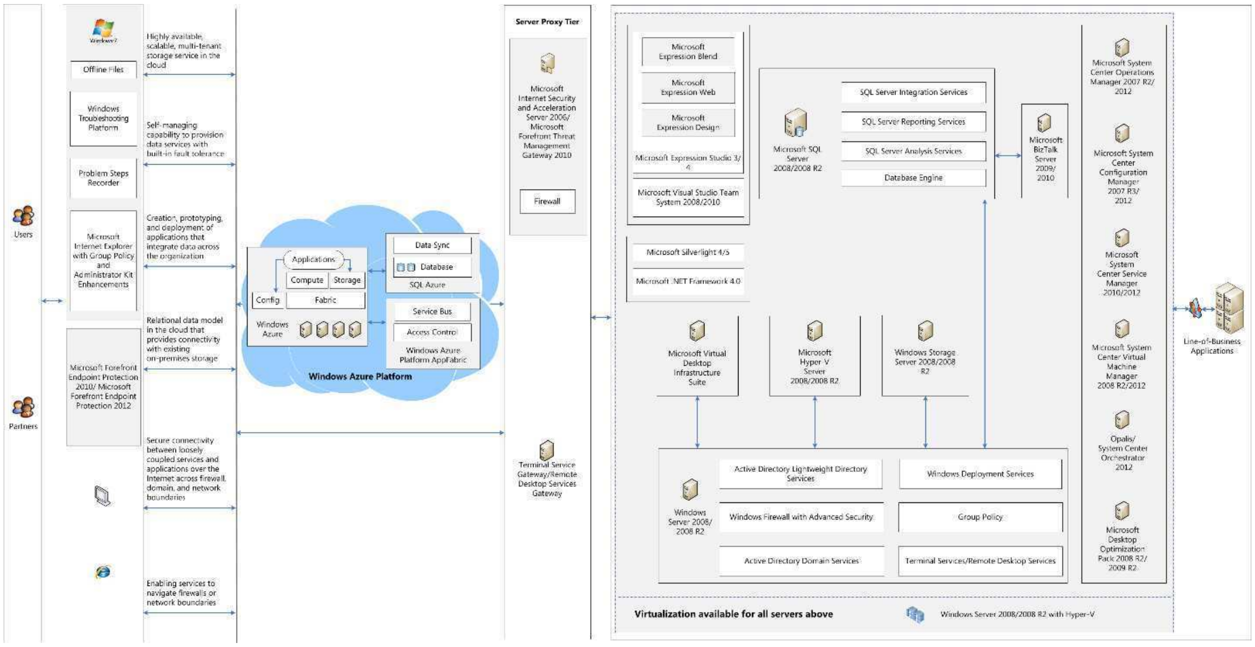
Azure Physical Design Phase 2


Users
Partners
Microsoft Outlook (RPC over HTTP/S)
Internet 802.11x—Hot Spots Broadband
HTTPS (443), SIP
Internet Cellular Network
HTTPS (443), SIP
Desktop Clients
Internet 802.11x—Hot Spots
Virtual Desktop Infrastructure/ Terminal Services Sessions/Remote Desktop Session via Remote Desktop Protocol
Router
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Microsoft Exchange Server 2007/2010 Role: Client Access, Edge Transport Server, Mailbox, Hub Transport Server, Unified Messaging
Terminal Services Gateway/ Remote Desktop Services Gateway
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Intelligent Application Gateway 2007/Forefront Unified Access Gateway 2010
Router
SIP/MTLS/5061
SIP/TLS/443
HTTPS (443)
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Microsoft Forefront Security for Exchange Server/Microsoft Forefront Protection 2010 for Exchange Server
Microsoft Office SharePoint Server 2007/Microsoft SharePoint Server 2010
Microsoft Exchange Server 2007/2010 Roles: Mailbox, Client Access, Edge Transport and Hub Transport, Unified Messaging
Microsoft Forefront Endpoint Protection 2010/Microsoft Forefront Endpoint Protection 2012
Microsoft BizTalk Server 2009/ 2010
Microsoft SQL Server 2008/2008 R2 Database Server
Microsoft Forefront Security for SharePoint/Microsoft Forefront Protection 2010 for SharePoint
Microsoft Hyper-V Server 2008/2008 R2
Windows Server AppFabric
Microsoft Identity Lifecycle Manager 2007/Microsoft Forefront Identity Manager 2010
Microsoft Windows Storage Server 2008/2008 R2
Windows Server 2008/ 2008 R2 Windows Deployment Services Windows Firewall with Advanced Security Group Policy Terminal Services /Remote Desktop Services
Microsoft Virtual Desktop Infrastructure Suite
Windows Server 2008/2008 R2 Active Directory Domain Services Active Directory Rights Management Services Active Directory Federation Services Active Directory Lightweight Directory Services
Windows Server 2008/2008 R2 Internet Information Services 7.0/7.5 Network Access Protection
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Microsoft System Center Data Protection Manager 2010/ 2012
Opalis/ System Center Orchestrator 2012
Microsoft System Center Service Manager 2010/2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Microsoft Desktop Optimization Pack 2008 R2/2009 R2
Applications
Line-of-Business Applications
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform

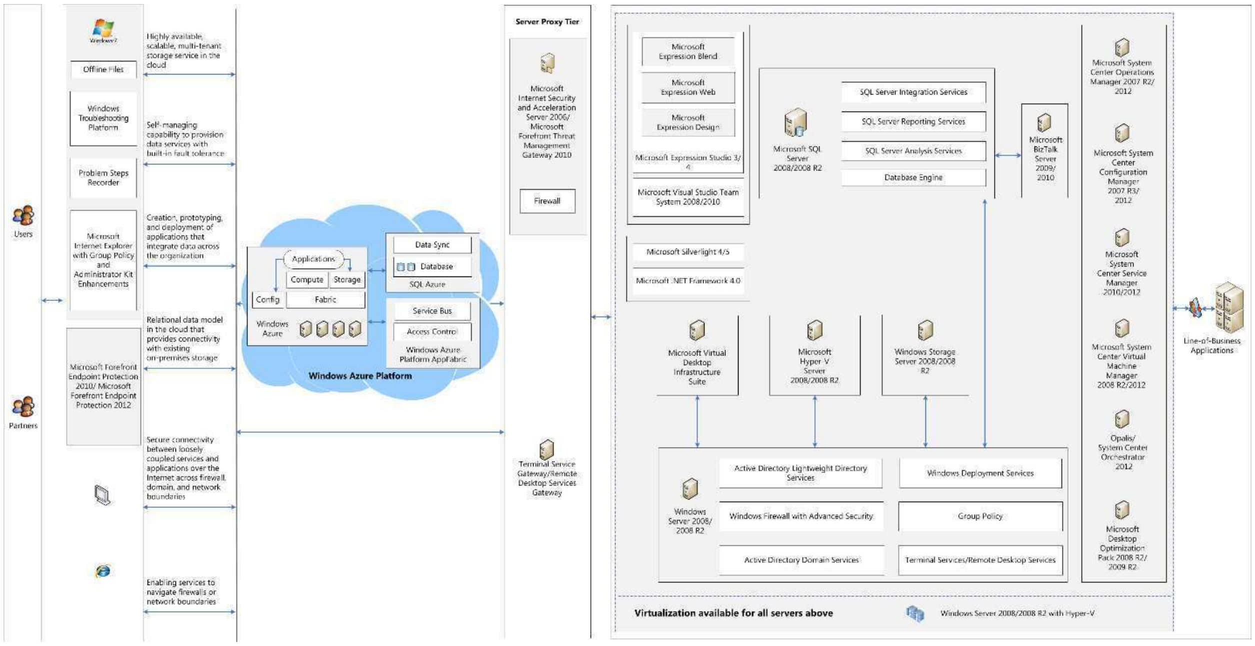
Azure Physical Design Phase 3


Users
Partners
Router
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Microsoft Forefront Security for Exchange Server/Microsoft Forefront Protection 2010 for Exchange Server
Microsoft Office SharePoint Server 2007/Microsoft SharePoint Server 2010
Microsoft Exchange Server 2007/2010 Roles: Mailbox, Client Access, Edge Transport and Hub Transport, Unified Messaging
Microsoft Forefront Endpoint Protection 2010/Microsoft Forefront Endpoint Protection 2012
Microsoft BizTalk Server 2009/2010
Microsoft SQL Server 2008/2008 R2 Database Server
Microsoft Forefront Security for SharePoint/Microsoft Forefront Protection 2010 for SharePoint
Microsoft Hyper-V Server 2008/2008 R2
Windows Server AppFabric
Microsoft Exchange Server 2007/ 2010 Role: Client Access, Edge Transport Server, Mailbox, Hub Transport Server, Unified Messaging
Terminal Services Gateway/ Remote Desktop Services Gateway
Microsoft Outlook (RPC over HTTP/S)
Internet 802.11x—Hot Spots Broadband
Internet Cellular Network
HTTPS (443), SIP
HTTPS (443), SIP
Microsoft Identity Lifecycle Manager 2007/Microsoft Forefront Identity Manager 2010
Microsoft Windows Storage Server 2008/2008 R2
Microsoft Forefront Server Security Management Console
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Intelligent Application Gateway 2007/Forefront Unified Access Gateway 2010
Windows Server 2008/2008 R2 Windows Deployment Services Windows Firewall with Advanced Security Group Policy Terminal Services/Remote Desktop Services
Microsoft Virtual Desktop Infrastructure Suite
Desktop Clients
Internet 802.11x—Hot Spots
Router
SIP/MTLS/5061
SIP/TLS/443
HTTPS (443)
Virtual Desktop Infrastructure/ Terminal Services Sessions/Remote Desktop Session via Remote Desktop Protocol
Windows Server 2008/2008 R2 Active Directory Domain Services Active Directory Rights Management Services Active Directory Federation Services Active Directory Lightweight Directory Services
Microsoft Internet Security and Acceleration Server 2006/Forefront Threat Management Gateway 2010
Microsoft Windows Server 2008/ 2008 R2 Internet Information Services 7.0/7.5 Network Access Protection
Microsoft Application Virtualization 4.5/ 4.6
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Microsoft System Center Data Protection Manager 2010/2012
Windows Embedded Device Manager 2011
Microsoft System Center Mobile Device Manager 2008
Opalis/System Center Orchestrator 2012
Microsoft System Center Service Manager 2010/2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Microsoft Desktop Optimization Pack2008 R2/2009 R2
Applications
Line-of-Business Applications
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform

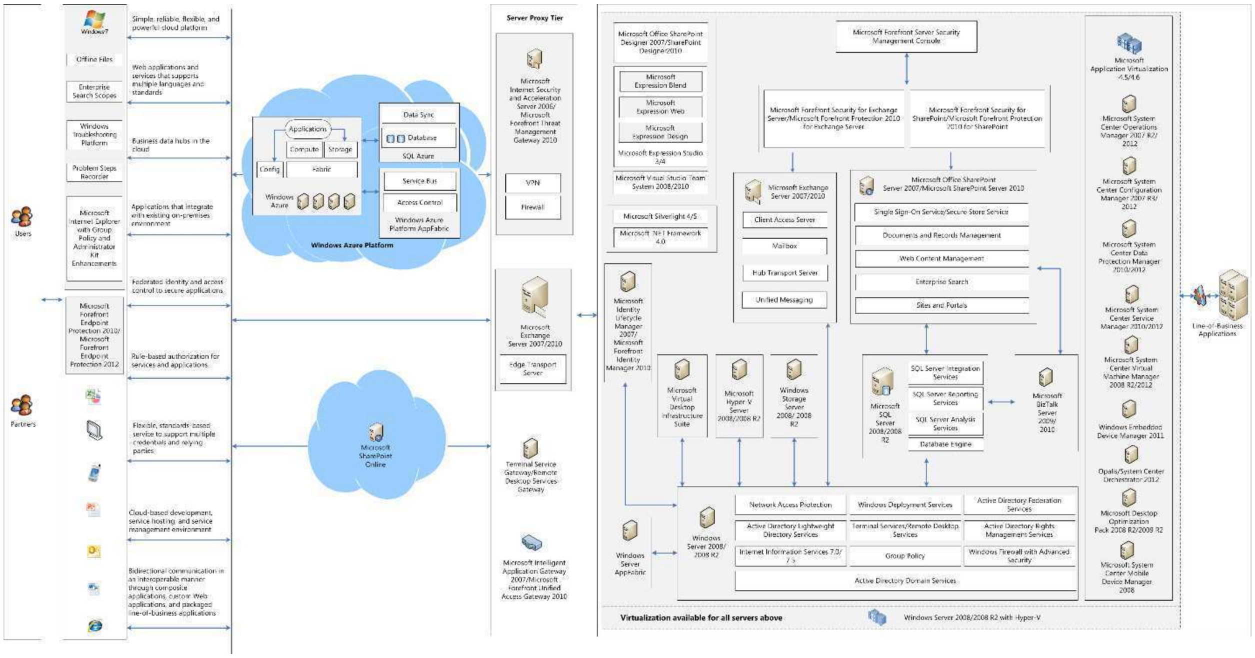
Azure Logical Design Phase 1


Windows7
Offline Files
Windows Troubleshooting Platform
Problem Steps Recorder
Microsoft Internet Explorer with Group Policy and Administrator Kit Enhancements
Microsoft Forefront Endpoint Protection 2010/ Microsoft Forefront Endpoint Protection 2012
Users
Partners
Highly available, scalable, multi-tenant storage service in the cloud
Self-managing capability to provision data services with built-in fault tolerance
Creation, prototyping, and deployment of applications that integrate data across the organization
Relational data model in the cloud that provides connectivity with existing on-premises storage
Secure connectivity between loosely coupled services and applications over the Internet across firewall, domain, and network boundaries
Enabling services to navigate firewalls or network boundaries
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform
Server Proxy Tier
Microsoft Internet Security and Acceleration Server 2006/ Microsoft Forefront Threat Management Gateway 2010
Firewall
Terminal Service Gateway/Remote Desktop Services Gateway
Microsoft Expression Blend
Microsoft Expression Web
Microsoft Expression Design
Microsoft Expression Studio 3/ 4
Microsoft Visual Studio Team System 2008/2010
Microsoft Silverlight 4/5
Microsoft .NET Framework 4.0
Microsoft SQL Server 2008/2008 R2
SQL Server Integration Services
SQL Server Reporting Services
SQL Server Analysis Services
Database Engine
Microsoft BizTalk Server 2009/ 2010
Microsoft Virtual Desktop Infrastructure Suite
Microsoft Hyper V Server 2008/2008 R2
Windows Storage Server 2008/2008 R2
Windows Server 2008/ 2008 R2
Active Directory Lightweight Directory Services
Windows Deployment Services
Windows Firewall with Advanced Security
Group Policy
Active Directory Domain Services
Terminal Services/Remote Desktop Services
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Microsoft System Center Service Manager 2010/2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Opalis/ System Center Orchestrator 2012
Microsoft Desktop Optimization Pack 2008 R2/ 2009 R2
Line-of-Business Applications
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V

Azure Logical Design Phase 2


Users
Partners
Windows7
Offline Files
Windows Troubleshooting Platform
Problem Steps Recorder
Microsoft Internet Explorer with Group Policy and Administrator Kit Enhancements
Microsoft Forefront Endpoint Protection 2010/ Microsoft Forefront Endpoint Protection 2012
Highly available, scalable, multi-tenant storage service in the cloud
Self-managing capability to provision data services with built-in fault tolerance
Creation, prototyping, and deployment of applications that integrate data across the organization
Relational data model in the cloud that provides connectivity with existing on-premises storage
Secure connectivity between loosely coupled services and applications over the Internet across firewall, domain, and network boundaries
Enabling services to navigate firewalls or network boundaries
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform
Server Proxy Tier
Microsoft Internet Security and Acceleration Server 2006/ Microsoft Forefront Threat Management Gateway 2010
Firewall
Terminal Service Gateway/Remote Desktop Services Gateway
Microsoft Expression Blend
Microsoft Expression Web
Microsoft Expression Design
Microsoft Expression Studio 3/ 4
Microsoft Visual Studio Team System 2008/2010
Microsoft Silverlight 4/5
Microsoft .NET Framework 4.0
Microsoft SQL Server 2008/2008 R2
SQL Server Integration Services
SQL Server Reporting Services
SQL Server Analysis Services
Database Engine
Microsoft BizTalk Server 2009/ 2010
Microsoft Virtual Desktop Infrastructure Suite
Microsoft Hyper V Server 2008/2008 R2
Windows Storage Server 2008/2008 R2
Windows Server 2008/ 2008 R2
Active Directory Lightweight Directory Services
Windows Deployment Services
Windows Firewall with Advanced Security
Group Policy
Active Directory Domain Services
Terminal Services/Remote Desktop Services
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Microsoft System Center Service Manager 2010/2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Opalis/ System Center Orchestrator 2012
Microsoft Desktop Optimization Pack 2008 R2/ 2009 R2
Line-of-Business Applications
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V

Azure Logical Design Phase 3


Users
Partners
Windows7
Offline Files
Enterprise Search Scopes
Windows Troubleshooting Platform
Problem Steps Recorder
Microsoft Internet Explorer with Group Policy and Administrator Kit Enhancements
Microsoft Forefront Endpoint Protection 2010/ Microsoft Forefront Endpoint Protection 2012
Simple, reliable, flexible, and powerful cloud platform
Web applications and services that supports multiple languages and standards
Business data hubs in the cloud
Applications that integrate with existing on-premises environment
Federated identity and access control to secure applications
Rule-based authorization for services and applications
Flexible, standards-based service to support multiple credentials and relying parties
Cloud-based development, service hosting, and service management environment
Bidirectional communication in an interoperable manner through composite applications, custom Web applications, and packaged line-of-business applications
Applications
Compute
Storage
Config
Fabric
Windows Azure
Data Sync
Database
SQL Azure
Service Bus
Access Control
Windows Azure Platform AppFabric
Windows Azure Platform
Microsoft SharePoint Online
Server Proxy Tier
Microsoft Internet Security and Acceleration Server 2006/ Microsoft Forefront Threat Management Gateway 2010
VPN
Firewall
Microsoft Exchange Server 2007/2010
Edge Transport Server
Terminal Service Gateway/Remote Desktop Services Gateway
Microsoft Intelligent Application Gateway 2007/Microsoft Forefront Unified Access Gateway 2010
Microsoft Office SharePoint Designer 2007/SharePoint Designer2010
Microsoft Expression Blend
Microsoft Expression Web
Microsoft Expression Design
Microsoft Expression Studio 3/4
Microsoft Visual Studio Team System 2008/2010
Microsoft Silverlight 4/5
Microsoft .NET Framework 4.0
Microsoft Identity Lifecycle Manager 2007/ Microsoft Forefront Identity Manager 2010
Microsoft Forefront Server Security Management Console
Microsoft Forefront Security for Exchange Server/Microsoft Forefront Protection 2010 for Exchange Server
Microsoft Forefront Security for SharePoint/Microsoft Forefront Protection 2010 for SharePoint
Microsoft Exchange Server 2007/2010
Client Access Server
Mailbox
Hub Transport Server
Unified Messaging
Microsoft Office SharePoint Server 2007/Microsoft SharePoint Server 2010
Single Sign-On Service/Secure Store Service
Documents and Records Management
Web Content Management
Enterprise Search
Sites and Portals
Microsoft Virtual Desktop Infrastructure Suite
Microsoft Hyper-V Server 2008/2008 R2
Windows Storage Server 2008/ 2008 R2
Microsoft SQL Server 2008/2008 R2
SQL Server Integration Services
SQL Server Reporting Services
SQL Server Analysis Services
Database Engine
Microsoft BizTalk Server 2009/ 2010
Windows Server AppFabric
Windows Server 2008/ 2008 R2
Network Access Protection
Windows Deployment Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Terminal Services/Remote Desktop Services
Active Directory Rights Management Services
Internet Information Services 7.0/ 7.5
Group Policy
Windows Firewall with Advanced Security
Active Directory Domain Services
Microsoft Application Virtualization 4.5/4.6
Microsoft System Center Operations Manager 2007 R2/ 2012
Microsoft System Center Configuration Manager 2007 R3/ 2012
Microsoft System Center Data Protection Manager 2010/2012
Microsoft System Center Service Manager 2010/2012
Microsoft System Center Virtual Machine Manager 2008 R2/2012
Windows Embedded Device Manager 2011
Opalis/System Center Orchestrator 2012
Microsoft Desktop Optimization Pack 2008 R2/2009 R2
Microsoft System Center Mobile Device Manager 2008
Line-of-Business Applications
Virtualization available for all servers above
Windows Server 2008/2008 R2 with Hyper-V

7 ORGANIZATION AND STAFFING

7.1 CONTRACT MANAGER

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

7.1.1

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

SHI Response:

Required Information	**Offeror's Response**
Name	Denise Verdicchio
Phone Number	908-884-1389
Email Address	Denise_Verdiccio@SHI.com
Position/Title	Senior Director, Public Sector
Years of industry experience	20 years in industry, 20 years with SHI
Work Hours	Standard Business work hours

7.1.2

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

SHI Response:

Dense Verdicchio has spent 20 years in the industry, and that entire time at SHI. Denise has held positions at SHI in Sales, Sales Management, and most recently, Denise was promoted to Senior Director for SHI's Public Sector field sales team across the country. As such, Denise has responsibility for all SHI Public Sector contracts. She has had experience managing many contracts of similar size and scope, and she is dedicated to excellence and continuous improvements in offerings and customer service.

Denise's resume follows:

Denise Verdicchio

908.884.1389
denise_verdicchio@SHI.com

202 Gregory Lane
Branchburg, NJ 08876

Senior Sales Professional / Account Manager

Offering 20 years of experience and achievement in the sale of IT software, hardware, and professional services to diverse business, healthcare, and government entities.

- Top sales performer with remarkable talent for connecting with customers, influencing key decision makers, and matching buyer needs with the right products to ensure ongoing satisfaction and repeat business.

- Assertive and resolute in pursuing opportunities, closing deals, resolving issues, and collaborating with vendors and other partners on seamless, timely implementation of world-class solutions.

- Knowledgeable and articulate in interfacing with clients and in delivering high-impact presentations that drive audiences to desired action. Accustomed to communicating with CEOs, CIOs, CTOs and other senior staff.

- Inspirational, empowering leader able to guide sales teams to unprecedented results; exceptionally organized in multitasking, keeping accounts up to date, and giving proper attention to multiple, concurrent deals.

- Passionate, enthusiastic, and hardworking. Driven each day to advance company goals, grow market share, surpass revenue targets, and boost bottom line profits while consistently exceeding client expectations.

- 7-time President's Club recipient, 3-time Chairwoman's Club designation, and Bali Award winner.

Career History

SHI International, Somerset, NJ, 1995 to Present

In a series of increasingly responsible roles, develop new business, exceed sales targets, and provide outstanding service to customers of this $6B global provider of innovative IT products and services.

Senior Director Public Sector, 7/1/2015-Present

Senior sales executive with 20 year accomplished career known for delivering and sustaining Revenue and profit gains within highly competitive market. Lead $1.3B business unit including team of 6 regional directors and 100 Account Executives in all aspects of sales, service, business

DEVELOPMENT, ACCOUNT MANAGEMENT, SOLUTIONS IMPLEMENTATION, AND ISSUE RESOLUTION ACROSS NORTH AMERICA. COLLABORATIVE LEADERSHIP STYLE INCLUDING ONGOING PERSONALIZED COACHING TO OTHER TEAM MEMBERS, OPEN INFORMATION SHARING, AND NURTURING CULTURE RESULTING IN CREATIVE AND INNOVATIVE ENVIRONMENT. EXCEPTIONAL COMMUNICATOR WITH CONSULTATIVE SALES STYLE, STRONG NEGOTIATION SKILLS, EXCEPTIONAL, EXCEPTIONAL PROBLEM SOLVING ABILITIES, AND A KEEN CLIENT NEEDS ASSESSMENT APTITUDE.

- SKILLED IN SENIOR-LEVEL PRESENTATIONS, NEGOTIATIONS, AND RELATIONSHIP BUILDING
- MAINTAIN KNOWLEDGE AND EXPERTISE OF TECHNOLOGIES INCLUDING END USER COMPUTING, DATACENTER, AND SECURITY
- DEVELOP AND IMPLEMENT SHORT AND LONG TERM SALES AND BUSINESS PLANS
- PROVIDE LEADERSHIP AND INNOVATION IN KEY ACCOUNT DEVELOPMENT AND MANAGEMENT
- ACKNOWLEDGED FOR EXCEPTIONAL STAFF DEVELOPMENT, MOTIVATION, AND TEAM BUILDING

Director – East Region SLED, 8/2013 to 6/30/2015

Lead team of 17 Account Executives in all aspects of sales, service, business development, account management, solutions implementation, and issue resolution for 8-state territory, SHI's largest region representing over $200M in annual revenue. Oversee daily operations in assisting customers with software and hardware procurement and implementation, system configuration, data center optimization, cloud computing, IT asset management, and various other computing solutions—ultimately helping clients maximize their IT investments and run successful businesses. Aggressively pursue new business through cold calling and other strategies. Travel extensively to client sites to provide in-person client support or drive new business opportunities. Partner with IT vendors and strategic partners on solutions implementation and in planning strategies to increase business.

- Excel in delivery of informative, insightful sales presentations to CEOs, CIOs, CTOs, CFOs, and other IT and procurement staff to update on current business and / or explain what SHI can do for them.
- Consistently demonstrate tremendous organization in keeping accounts current, overseeing all deals from 12 Account Executives, and responding to up to 400 customer emails daily.
- Motivate teams each day to work to their full potential. Provide ongoing coaching and support.
- Promoted to Director after highly successful tenure as Account Executive.

SHI INTERNATIONAL, Somerset, NJ

Account Executive – NJ State and Local Government, 2010 to Present

Develop new business, service customer needs, and oversee daily account management for public sector clients in NJ State and Local Government. Interface daily with customers in providing information, resolving issues, communicating SHI offerings, and enabling them to secure quotes through their own procurement systems. Negotiate deals, support customer contracts, and deliver sales presentations. Onboard new vendors, enabling them to procure software on the NJ state contract. Collaborate with vendors on delivery of comprehensive IT solutions.

- Grew this new line of business from $0 to $40M in three years, establishing all new clients--including 19 NJ counties, more than 100 individual townships, and all state agencies.
- Delivered more than $2M in cost savings to clients through successful price negotiations with vendors.
- Regularly exceed quarterly / annual sales targets.

SHI INTERNATIONAL, Somerset, NJ

Account Executive – North Carolina Commercial Accounts, 1998 to 2010

Orchestrated customized, total IT solutions for Duke Energy (30K employees), SAS Institute, Wake Forest University, and other commercial accounts throughout North Carolina. Aggressively pursued and developed new business through cold calling, networking, and other forms of outreach.

- Fostered and fortified strong, mutually beneficial relationships with Microsoft, Adobe, Symantec, McAfee, HP, VMware, Amazon Web Service, EMC, Lenovo, and other strategic partners.
- Demonstrated tremendous energy and unyielding commitment to being in front of customers as often as possible to create and expand relationships.

~ Earlier SHI experience as **Human Resources Assistant** (1997 to 1998), hiring employees to all SHI divisions; and as **Inside Account Manager** (1995 to 1997), answering customer calls, quoting product, placing orders, and providing support to North Carolina accounts. ~

Education

Bachelor of Arts Degree in Psychology and Sociology
RUTGERS COLLEGE, New Brunswick, NJ
Double Major; Honor's Graduate

Professional Development:
Microsoft Sales Professional Certification • VMWare Sales Specialist •
McAFee Certified Sales Professional

7.1.3

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

SHI Response:

As SHI's Senior Director for Public Sector, Denise not only will take personal responsibility for the management of this contract, she also has access to and control over a wide variety of resources within SHI to ensure the success of this contract.

Denise understands the intracacies of implementing and maintaining a contract of this nature, supporting multiple state agencies and municipalities. When SHI enters into an agreement of this magnitude, we take great care to implement support and service plans to meet the needs of each State, while also supporting each indivual agency, city, county, township, school district and higher education institution.

While Denise will act as the Contract Manager and Single Point of Contact for this contract, she is certainly not alone in the support of this contract. Denise will coordinate the efforts of SHI's contracts team, our Solutions specialists, our Public Sector Marketing team, and of course our Public Sector sales team across the country.

To give you an idea of our scope of coverage from a sales perspective, SHI is proud to support our Public Sector customers with the following team members who work *exclusively with Public Sector*:

- 88 Field Account Executives supporting State & Local Government and Education
- 150 Inside Account Executives supporting Small/Medium Local Government and Education customers
- 94 Inside Account Managers who partner with our Field Account Executives and assist customers with their day to day quoting and ordering needs
- 7 Public Sector Marketing Managers who are dedicated to support the success of our sales team

In short, SHI has many representatives who will support the NASPO ValuePoint SVAR contract both within our Headquarters office and across the country. Denise looks forward to coordinating all of these resources to the maximum benefit of NASPO ValuePoint and each Participating State.

8 TECHNICAL REQUIREMENTS

If applicable to an Offerors offering, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's offering then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For Section 8 we have provided the response from each of these partners.

8.1 TECHNICAL REQUIREMENTS

8.1.1

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

AWS Response:

Our proposed service models are IaaS and PaaS, each deployed in either Community, Public or Hybrid models. Our proposed IaaS and PaaS cloud offers have the ability to store and secure Low, Moderate and High Risk data in conformance with FIPS designations.

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

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 you provision and use what you need via a web application. All AWS cloud services are driven by robust APIs that allow for a wide variety of monitoring and management tools to integrate easily with AWS cloud resources. Common tools from vendors such as Microsoft, VMware, BMC Software, Okta, RightScale, Eucalyptus, CA, Xceedium, Symantec, Racemi, and Dell already support AWS, to name just a few. This flexibility allows AWS customers to easily provision, manage, and monitor all of their IT resources through a “single pane of glass” with the tool that best fits their unique needs. This also means a full inventory of those resources is only a few clicks away.

- **Management Console:** The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS regions and lets customers provision resources across multiple regions.
- **Command Line Interface:** The AWS Command Line Interface (CLI) is a unified tool used to manage AWS cloud services. With just one tool to download and configure, customers can control multiple AWS resources from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon Simple Storage Service (Amazon S3).

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

- AWS Management Portal for vCenter enables customers to manage their AWS resources using VMware vCenter. The portal installs as a vCenter plug-in within the existing vCenter environment. Once installed, it enables customers to migrate VMware VMs to Amazon EC2 and manage AWS resources from within vCenter. The AWS resources that customers create using the portal can be located in their AWS account, even though those resources have been created using vCenter. For experienced VMware administrators, AWS Management Portal for vCenter provides a familiar look and feel that can make it easy to start using AWS. AWS Management Portal for vCenter is available at no additional charge.
- The Amazon EC2 VM Import Connector extends the capabilities of VMware vCenter to provide a familiar graphical user interface customers can use to import their preexisting Virtual Machines (VMs) to Amazon EC2. Using the connector, importing a VM is as simple as selecting a VM from the vSphere infrastructure, and specifying the AWS region, Availability Zone, operating system, instance size, security group, and Amazon Virtual Private Cloud (Amazon VPC) details (if desired) into which the VM should be imported. Once the VM has been imported, customers can launch it as an instance from the AWS Management Console and immediately take advantage of all the features of Amazon EC2.
- AWS Management Pack for Microsoft System Center enables customers to view and monitor their AWS resources directly in the Operations Manager console. This way, customers can use a single, familiar console to monitor all of their resources, whether they are on-premises or in the AWS cloud. You get a consolidated view of all AWS resources across regions and Availability Zones. It also has built-in integration with Amazon CloudWatch so that the metrics and alarms defined in Amazon CloudWatch surface as performance counters and alerts in the Operations

Manager console. Information on AWS Management Pack for Microsoft System Center can be found here.

Rapid Elasticity

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

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 customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010.

Measured Service

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

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

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

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

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

AWS publishes these reports up to several times a day in comma-separated value (CSV) format to an Amazon S3 bucket that you specify. After you set up your account to receive detailed billing reports in an Amazon S3 bucket, AWS starts to write reports to the bucket several times each day. You can get these reports using the Amazon S3 console, application programming interface (API), and command line interface (CLI). The file contains charges for the account, broken down by AWS product and individual type of usage.

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

AWS Budgets: You can define a monthly budget for your AWS costs—whether at an aggregate cost level (i.e., “all costs”) or further refined to include only those costs relating to specific cost dimensions or groups of cost dimensions, including Linked Account, Service, Tag, Availability Zone (“AZ”), Purchase Option (e.g., Reserved), and/or API Operation.

Further, you can attach email notifications to these budgets that are triggered when your actual or forecasted costs exceed a threshold—that you define—relative to your budgeted costs. For example, you could create a monthly budget titled “Monthly Marketing Budget – EC2” and include within it only those costs relating to EC2 that you have tagged “Department:Marketing.” You could then elect to receive email notifications when your actual costs exceed 80% of your budgeted costs or when your forecasted costs exceed 100% of your budgeted costs. All of your budgets are available for viewing within the Budgets Dashboard—complete with detailed data (e.g., budget dimensions and time range) and variance analyses—and within Cost Explorer.

Full information on AWS billing can be found on the AWS website: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/DetailedBillingReports.html.

Hybrid Model (Extend IT Services)

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

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

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

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

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

- **Extend Network Configuration**: Flexible network connectivity is a cornerstone of integrating distributed environments, including AWS and your existing on-premises equipment. With Amazon VPC, you can extend your on-premises network configuration into your virtual private networks on the AWS cloud. AWS resources can operate as if they are part of your existing corporate network. Amazon VPC lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- **Integrated Cloud Backups**: AWS helps simplify the backup and recovery environment for the enterprise. You can leverage the on-demand nature of the cloud and automate your backup and recovery processes so they are not only less complex and lightweight, but also easy to manage and maintain. Storage services with AWS are designed to provide 99.999999999% durability, so you can feel confident your backups are protected.
- **Integrated Network Connection**: On-premises connection with AWS is best accomplished with AWS Storage Gateway, a software appliance installed in your data center with cloud-based storage to provide seamless and secure integration between an organization's existing IT environment and the AWS storage infrastructure. Using industry-standard storage protocols, the service allows you to store data in the AWS cloud for scalable and cost-effective storage. It provides low-latency performance by maintaining frequently accessed data on-premises while securely storing all of your data encrypted in the Amazon Simple Storage Service (Amazon S3) or Amazon Glacier.
- **Integrated Resource Management and Workload Migration**: All AWS cloud services are driven by robust APIs that allow for a wide variety of monitoring and management tools that integrate easily with your AWS cloud resources. It's likely that many of the tools that your organization is using to manage your on-premises environments can be extended to include AWS as well. Integrating your AWS environment can provide a simpler and quicker path for cloud adoption, because your operations team does not need to learn new tools or develop completely new processes.

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

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

Hybrid Cloud Resources: AWS provides the tools, information, and guidance to build a hybrid cloud environment that can offer an immediate impact to customers. Visit our hybrid cloud webpage for information on how to get started: http://aws.amazon.com/enterprise/hybrid/

CA Response:

Agile - CA Agile Central is a SaaS offering that is generally used to document and manage work within the SDLC.

APIM – CA APIM SaaS offering helps accelerate, secure and manage APIs. CA is responsible for development and management of application. AWS provides IaaS services to CA for management of the underlying cloud infrastructure.

ASM - CA App Synthetic Monitor (ASM) provides end-to-end transaction response-time visibility into cloud, mobile and Web applications. Application utilizes Rack Space IaaS services.

MAA – CA Mobile App Analytics stimulates collaboration between business analysts, developers, operations and support in order to accelerate mobile app delivery and improve end-user experience. This service is hosted at CenturyLink Data center and the infrastructure is managed and maintained by CA SaaS Ops and Delivery team.

PPM – Project Portfolio Management represents a single platform that enables you to manage your entire innovation lifecycle and make more informed strategic investments. CA PPM helps you track and prioritize market and customer requirements and make better decisions on how to invest limited resources.

Microsoft Response:

See the response to question 6.7.

8.1.2

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

8.1.2.1 NIST Characteristic - On-Demand Self-Service:

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

AWS Response:

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

CA Response:

Agile - CA Agile Central is a SaaS offering that is generally used to document and manage work within the SDLC.

APIM – N/A. This is a SaaS service and clients do not have direct access to the underlying infrastructure in order to provision computing capabilities. CA is responsible for the management and maintenance of the infrastructure and will make any necessary adjustments as part of providing this service to its clients.

ASM – This does not apply as this is a SaaS service. ASM customers are able to manage all aspects of their accounts, create sub-accounts, and make any configuration changes necessary for their monitors.

MAA – This is a SaaS offering and On-Demand service is not available, however, MAA customers are enabled to manage their accounts and carry out configuration changes required to manage mobile applications.

PPM – Each PPM SaaS instance is provisioned to support the users subscribed to it. Additional storage and compute resources are provided as required without client action. Clients have the capability to provision users and define access in a self-service model

Microsoft Response:

Microsoft Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money. Azure serves as a development, service hosting, and service management environment, providing customers with on-demand compute, storage, networking, and content delivery capabilities to host, scale, and manage applications on the Internet.

8.1.2.2 NIST Characteristic - Broad Network Access:

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

AWS Response:

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

CA Response:

Agile - All access to the application is through a browser.

APIM – The APIM service is accessed via HTTPS on a supported browser with no requirements for a workstation client install; mobile friendly and optimized for use with iOS and Android tablets

ASM – The ASM dashboard and API are accessible from any host connected to the public Internet. The API and dashboard require authentication, and each account is only accessible by the account owner (customer).

MAA – Upon native authentication, MAA dashboard is accessible by any host over public internet. Also, mobile devices connect to the service using REST API.

PPM – The PPM service is accessed via HTTPS on a supported browser with no requirements for a workstation client install.

Microsoft Response:

An Azure virtual network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. You can fully control the IP address blocks, DNS settings, security policies, and route tables within this network. You can also further segment your VNet into subnets and launch Azure IaaS virtual machines (VMs) and/or Cloud services (PaaS role instances). Additionally you can connect the virtual network to your on-premises network using one of the connectivity options available in Azure. In essence, you can expand your network to Azure, with complete control on IP address blocks with the benefit of enterprise scale Azure provides.

8.1.2.3 NIST Characteristic - Resource Pooling:

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

AWS Response:

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010.

CA Response:

Agile - We monitor all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. We can easily scale our systems to accommodate any additional capacity. If we determine a single user is using a significant amount of resources we will proactively reach out to them to understand what they are trying to accomplish and help them to formulate more performant queries.

APIM – CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon's infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.

ASM – All ASM core servers are dedicated physical servers. ASM Public Status Pages are served from dedicated web servers (used only by CA ASM) in the Amazon Cloud, on shared tenancy virtualization. Amazon Cloud virtual machines used by ASM are managed by and provisioned by CA ASM systems administrators.

MAA – MAA core service utilizes dedicated infrastructure layered with virtualization capabilities. It doesn't share computing resources with other services. Tenants are segregated using application containerization capabilities.

PPM – For US based clients a scalable service is provided based solely within the US. Clients are provided with dedicated compute resources and pooled network/ISP which are monitored and adjusted to insure performance.

Microsoft Response:

Azure Resource Manager enables you to deploy and manage your solutions through resource groups. Typically, a resource group contains resources related to a specific application. For example, a group may contain a web app that hosts your public website, a SQL Database that stores relational data used by the site, and a Storage account that stores non-relational assets. Every resource in a resource group should share the same lifecycle. For more information about Resource Manager, see Resource Manager overview.

Currently, not every service supports the portal or Resource Manager. For those services, you will need to use the classic portal. For the status of each service, see Azure portal availability chart.

You can also manage resources through Azure PowerShell and Azure CLI. For more information about using those interfaces, see Using Azure PowerShell with Azure Resource Manager and Use the Azure CLI for Mac, Linux, and Windows with Azure Resource Manager.

8.1.2.4 NIST Characteristic - Rapid Elasticity:

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

AWS Response:

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

CA Response:

Agile - This is a SaaS service, therefore, CA monitors all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. Data storage and network capacity are monitored and scaled to meet current client demands. Compute resources are scaled to meet client processing requirements

APIM – CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon’s infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.

ASM – All ASM core servers are dedicated physical servers; there is no elasticity. The ASM Public Status Pages are served from web servers in the Amazon Cloud, and the pool of web servers can be grown or shrunk if necessary. Any changes to the size of the pool would be transparent to end-users and customers, and would only be done by CA ASM systems administrators. Since this is a SaaS environment the CA SaaS Operations and delivery along with RackSpace are responsible for management of the capacity and monitoring.

MAA – The pool of web and application servers can be grown or shrunk when necessary. Any changes to the size of the pool remains transparent to end-users and customers, and would only be done by CA MAA systems administrators.

PPM – Data storage and network capacity are monitored and scaled to meet current client demands. Compute resources are scaled to meet client processing requirements.

Microsoft Response:

Azure provide the ability to manually scale your application or set parameters to automatically scale it. Azure offers the ability to scale applications that are running Web Roles, Worker Roles, or Virtual Machines. To scale an application that is running instances of Web Roles or Worker Roles, you add or remove role instances to accommodate the work load.

When scaling an application up or down that is running Virtual Machines, new machines are not created or deleted, but are turned on or turned off from an availability set of previously created machines. Scaling can be based on average percentage of CPU usage or based on the number of messages in a queue.

Please consider the following information before you configure scaling for your application:

- You must add Virtual Machines that you create to an availability set to scale an application that uses them. The Virtual Machines that you add can be initially turned on or turned off, but they will be turned on in a scale-up action and turned off in a scale-down action. For more information about Virtual Machines and availability sets, see Manage the Availability of Virtual Machines.
- Scaling is affected by core usage. Larger role instances or Virtual Machines use more cores. You can only scale an application within the limit of cores for your subscription. For example, if your subscription has a limit of twenty cores and you run an application with two medium sized Virtual Machines (a total of four cores), you can only scale up other cloud service deployments in your subscription by sixteen cores. All Virtual Machines in an availability set that are used in scaling an application must be the same size. For more information about core usage and machine sizes, see Virtual Machine and Cloud Service Sizes for Azure.
- You must create a queue and associate it with a role or availability set before you can scale an application based on a message threshold. For more information, see How to use the Queue Storage Service.
- You can scale resources that are linked to your cloud service. For more information about linking resources, see How to: Link a resource to a cloud service.
- To enable high availability of your application, you should ensure that it is deployed with two or more role instances or Virtual Machines. For more information, see Service Level Agreements.

8.1.2.5 NIST Characteristic – Measured Service:

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

AWS Response:

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

CA Response:

Agile - Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity

CA's best-of-breed monitoring solutions are deployed and supplemented with vendor specific diagnostic tools where appropriate

24x7 staffed network operation center (NOC) to analyze and respond to automated monitoring alerts

APIM – Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity. This portion is handled for the underlying cloud infrastructure by AWS with active participation by CA including escalations of issues.

ASM – CA ASM systems administrators track the resource consumption of each virtual machine in the cloud. Since this is a SaaS service, ASM customers do not need this information in order to use the service, nor do they have access to view it.

MAA – CA MAA systems administrators track the resource consumption of each virtual machine in use. ITIL flows are utilized to ensure service delivery. MAA customers do not need this information in order to use the service, nor do they have access to view it.

PPM – Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity
CA's best-of-breed monitoring solutions are deployed and supplemented with vendor specific diagnostic tools where appropriate 24x7 staffed network operation center (NOC) to analyze and respond to automated monitoring alerts

Microsoft Response:

By default, minimal monitoring is provided for a new cloud service using performance counters gathered from the host operating system for the roles instances (virtual machines). The minimal metrics are limited to CPU Percentage, Data In, Data Out, Disk Read Throughput, and Disk Write Throughput. By configuring verbose monitoring, you can receive additional metrics based on performance data within the virtual machines (role instances). The verbose metrics enable closer analysis of issues that occur during application operations.

By default performance counter data from role instances is sampled and transferred from the role instance at 3-minute intervals. When you enable verbose monitoring, the raw performance counter data is aggregated for each role instance and across role instances for each role at intervals of 5 minutes, 1 hour, and 12 hours. The aggregated data is purged after 10 days.

After you enable verbose monitoring, the aggregated monitoring data is stored in tables in your storage account. To enable verbose monitoring for a role, you must configure a diagnostics connection string that links to the storage account. You can use different storage accounts for different roles.

Note that enabling verbose monitoring will increase your storage costs related to data storage, data transfer, and storage transactions. Minimal monitoring does not require a storage account. The data for the metrics that are exposed at the minimal monitoring level are not stored in your storage account, even if you set the monitoring level to verbose.

8.1.3

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

SHI Response:

Our **IaaS** service model offers the following subcategories:

- Computer/Infrastructure Services
    - Operating systems
        - Windows
        - Linux
        - BSD
    - Dedicated Hosts
    - Xen Hypervisor
- Storage
    - File
    - Block
    - Object
    - Archive
    - Cache
    - Content Delivery Network (CDN)
- Network
    - Virtual network
    - Load balancer
    - DNS
    - Gateways via VPNs
    - Firewall
    - Traffic manager
    - Direct link
- PC/Desktop “aaS”

- Security
    - Identity & Access Management
    - Encryption
    - Network Security
    - Intrusion Management
    - DDOS Monitoring / Management

The following **IaaS** subcategories are supported if designed and provisioned by users:

- Disaster Recovery
    - Business Continuity
    - High Availability / Failover
- Security subcategories listed below are in addition to the native IaaS subcategories listed above:
    - Data Loss Prevention (DLP)
    - Web Security
    - Email Security
    - Security Information and Event Management (SIEM)

Our **PaaS** service model offers the following subcategories:

- Analytics
    - Hadoop
    - Business Intelligence
    - Data Warehouse
- Database
    - Relational
    - NoSQL
- Development, Testing and Deployment
    - Containers
    - Services and APIs
    - Mobile
    - Internet of Things
    - Tools
    - Runtime environments
- Open Source

CA Response:

Agile - We provide a SaaS offering that is generally used to document and manage work within the SDLC. In addition to the CA Agile offering CA Technologies also offers educational services and consultancy services.

APIM – In addition to the APIM SaaS offering CA Technologies also offers educational services and consultancy services. CA provides education and training services to its clients.

ASM – An ASM is a SaaS offering that provides customers with the ability to monitor the availability, health, and performance of network services (web sites, email servers, etc.).

MAA – CA MAA helps app developers visualize, investigate, manage, and support user interactions with their mobile apps. It provides deep insights into the performance, user experience, crash, and log analytics of mobile apps. CA MAA is aimed to help enterprises understand the experience of mobile app users across the DevOps application lifecycle. Enterprises can accelerate the delivery of user-experience-focused mobile applications and can achieve faster time to market by continuous application delivery while ensuring robust security.

PPM – In addition to the PPM SaaS offering CA Technologies also offers educational services and consultancy services.

Microsoft Response:

Microsoft Azure offers IaaS, Saas and PaaS offerings for Commercial, Education and Government entities.

8.1.4

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

SHI Response:

AWS Response:

Please see response to question 6.5.3 and 8.6.2.

CA Response:

Please see response to question 6.5.3 and 8.6.2.

Microsoft Response:

Please see response to question 6.5.3 and 8.6.2.

8.1.5

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

SHI Response:

The IaaS and PaaS services offered are designed to strictly support the NIST cloud definitions and functional delineations for each respective service model. The IaaS and PaaS implementations are audited to comply with numerous oversight entities, so that users are able to build architectures suitable for storing, processing and appropriate handling of Low, Moderate and High Risk data.

SHI is taking a flexible approach to this response in order to provide NASPO and NASPO Participating entities with the broadest offering of products over the life of this contract.

AWS

SHI has the flexibility to offer AWS Services directly to the customer or through a certified partner such as Day 1 Solutions. We will work with each customer on a case by case basis to determine which is the most cost effective and efficient method.

Microsoft

SHI will be reselling Microsoft products and services to NASPO Participating Entities.   SHI will handle all of the logistics for NASPO Entities – scoping, quoting, PO placement, licensing agreements, usage reports, and billing. SHI is Microsoft's number 1 partner in the Public Sector space and vast experience specifically with 0365 and Azure as well as other cloud based offerings.

CA

SHI will be reselling CA products and solutions to NASPO participating entities. SHI will work with each customer on a case by case basis to determine which is the most cost effective and efficient solution based on their needs.

8.2 SUBCONTRACTORS

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. Subcontractor do not need to comply with Section 6.3.

SHI Response:

SHI is taking a flexible approach to this response in order to provide NASPO and NASPO Participating entities with the broadest offering of products over the life of this contract.

AWS

SHI has the flexibility to offer AWS Services directly to the customer or through a certified partner such as Day 1 Solutions.   We will work with each customer on a case by case basis to determine which is the most cost effective and efficient method.

Microsoft

SHI will be reselling Microsoft products and services to NASPO Participating Entities.   SHI will handle all of the logistics for NASPO Entities – scoping, quoting, PO placement, licensing agreements, usage reports, and billing. SHI is Microsoft's number 1 partner in the Public Sector space and vast experience specifically with 0365 and Azure as well as other cloud based offerings.

CA

SHI will be reselling CA products and solutions to NASPO participating entities. SHI will work with each customer on a case by case basis to determine which is the most cost effective and efficient solution based on their needs. CA Technologies may use sub-contractors and will ensure that any such usage meets the security and other contractual requirements for the service being provided. CA Technologies retains responsibility for any activities performed by a subcontractor.

8.2.1

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.

SHI Response:

SHI will work hand in hand with each of the partners represented on this NASPO RFP response as well as any partners added in the future to meet the requirements of this RFP. The partners are a critical piece of this process as many of these products are usage based and the OEM holds that information. For Microsoft Azure, SHI may work with our elite partners that can offer additional services regarding Azure and specific to the customer requirements. Elite partners undergo an intensive vetting process to ensure that any work performed is on par with the standards SHI uses for their internal employees responsible for service delivery. Elite partners are required to fulfill statement of work requirements.

Any implementation or support services will also be delivered by the respective partner. SHI will work with our customers and partners to determine what the best path to these services are in each case. Most often we pass these through directly to the partner so the customer has immediate access to support when needed.

SHI can offer Project Management to our customers to ensure that migrations to the cloud happen efficiently and on time.

SHI is always available to our customers and can assist in directing our customers to the correct place for support.

For CA Agile, currently co-location data center operations are sub-contracted, however, all infrastructure is managed and maintained by CA as well as application development. Therefore, subcontractors do not have access to the Data.

For CA APIM, AWS is the IaaS provider, managing all aspects of the underlying cloud infrastructure.

For CA ASM, Rackspace provides IaaS services to provision processing, storage, networks, and other fundamental computing resources. CA manages the operating systems and all aspects of ASM applications.

For CA MAA and PPM - Currently co-location data center operations are sub-contracted, however, all infrastructure is managed and maintained by CA as well as application development. Therefore, subcontractors do not have access to the Data.

8.2.2

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.

SHI Response:

All of the partners that SHI has included in this RFP Response are known. Below you will find qualifications that demonstrate how they will meet the experience requirements of the RFP. SHI has created a partner package that includes all of the requirements set forth by NASPO. Each time we engage a new partner or subcontractor we will have that partner review and fill out the partner package to demonstrate that they meet or exceed NASPO requirements.

For CA Products, all subcontractors are vetted to meet the same or higher compliance standards as CA Technologies. All subcontractors are subjected to the annual SSAE16 audit and covered in the related report.

8.3 WORKING WITH PURCHASING ENTITIES

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

8.3.1

Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;

- ***Response times;***
- ***Processes and timelines;***
- ***Methods of communication and assistance; and***
- ***Other information vital to understanding the service you provide.***

AWS Response:

Data Breaches and other security vulnerabilities, either reported, actual incidents, or other events, are evaluated using CVSS v2. Impacted clients are notified directly via non-automated email within 24 hours, and at least every 5 days afterwards until resolved.

In addition to direct communication, security bulletins are disclosed publicly http://aws.amazon.com/security/security-bulletins/

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 standards, system utilities are appropriately restricted and monitored. Below is an outline of the three-phased approach AWS has implemented to manage incidents:

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

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

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

CA Response:

CA Technologies abides to contractual requirements for notification, in addition to working with legal to ensure compliance with regulatory requirements. There may be cases where incident analysis completion is a requirement for confirming the breach, and / or its impact and data leakage boundary.

Prior to completion of this activity, CA may not have the needed conclusions for customer communication. Once subscriber data has been identified as part of the investigation, said subscribers will be notified as soon as possible and not longer than 5 days. A report of the incident will be available and distributed to clients within 30 days.

Microsoft Response:

The Microsoft Azure trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures.

Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state.

Azure validates services using third party penetration testing based upon the OWASP (Open Web Application Security Project) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices.

Azure services staff suspected of committing breaches of security and/or violating the Information Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination.

Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts.

Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on secure infrastructure and are retained for 180 days.

Microsoft Identity Manager and intrusion detection system tools are implemented within the Azure environment. Azure uses an early warning system to support real-time analysis of security events within its operational environment. Monitoring agents and the alert and incident management system generate near real-time alerts about events that could potentially compromise the system.

Microsoft Azure has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things, unauthorized access resulting in loss, disclosure or alteration of data.

The Azure Incident Response process follows five main phases:

- Identification – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists.

- Containment – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices.
- Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If a vulnerability is determined, the escalation team reports the issue to product engineering.
- Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity.
- Lessons Learned – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.

In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, impacted customers (tenants) and/or other external business relationships of a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.

Security incident response plans and collection of evidence adheres to ISO 27001 standards. MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the TSG are followed.

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.

AWS Response:

AWS services are provisioned on-demand by the customer; this is the passive nature of IaaS. The customer controls how it uses its account and what content moves onto and off of its account. AWS SOC reports (available under AWS NDA) provide additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. Neither SHI nor AWS are agents of or otherwise engaged in advertising via advertising networks, adware, procured software or other such marketing entities.

CA Response:

CA Technologies hosts all of its SaaS Offerings in a secure private data center, and does not allow third-party marketing or content providers to inject any content into the customer's session. No Advertising, software or any additional content of any type is allowed by CA policies and controls.

Microsoft Response:

Microsoft Azure does not provide e-commerce solutions.

Note that Customer Data will be used only to provide customer the Microsoft Azure service. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

More information on Microsoft's commitment around use of customer data can be found in the Privacy Statement and Online Services Use Rights

8.3.3

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

AWS Response:

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

CA Response:

CA has the ability to provide its customers with a test/staging environment that is identical to production with the possible exception of capacity. CA works with its clients on a case-by-case basis to provide the appropriate level of testing/staging environment based on needs and requirements.

Microsoft Response:

Azure has the capability of both staging and production environments for the services offered. Environments can be created via Azure credits provided through all MSDN subscriptions in addition to the Azure DevTest Labs feature which is now in preview.

8.3.4

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

AWS Response:

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

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

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

AWS provides API-based cloud computing services with multiple interfaces to those services, including SDKs, IDE Toolkits, and Command Line Tools for developing and managing AWS resources. In addition, AWS provides two graphical user interfaces, the AWS Management Console and the AWS ElasticWolf Client Console. The AWS ElasticWolf Client Console has incorporated Section 508 requirements and AWS has prepared a Voluntary Product Accessibility Template (VPAT) for the Console, which outlines the Console's accessibility features.

CA Response:

A CA licensed program that has been evaluated by us for Section 508 purposes will have a Voluntary Product Accessibility Template ("VPAT"). CA evaluates such licensed programs consistent with the standards of the Information Technology Industry Council ("ITIC"). CA's evaluation of each such licensed program is recorded on the standardized VPAT template developed by ITIC. The VPAT identifies how each evaluated licensed program does or does not meet the Section 508 requirements, or provides functional equivalence ("Functional Equivalence"), as set forth in the Section 508 regulations.

As part of the post-contract maintenance and support to be provided to its licensees under any agreement, CA will provide Section 508 upgrades and enhancements, Section 508 Functional Equivalence or other Section 508 deliverables referenced in any VPAT ("Section 508 Upgrades and Enhancements") on a when and if-available basis, comprised of error-corrections, patches, work-arounds, and additional features and functionality which are within the domain of, and which will not replace, the underlying CA licensed program.

CA is not aware of any requirement under Section 508 that governs professional IT services beyond traditional software support. CA Services does not make any representation or warranty regarding whether any work it performs under this agreement will affect the accessibility of any generally available CA Software product. Should the Government require CA Services to develop, modify and/or deliver code or other work product in the course of performing under this agreement, CA does not represent or warrant that such code or work product will be independently compliant with Section 508. A copy (CA PPM only) can be requested by calling 1-800-225-5224.

Microsoft Response:

The Microsoft Product Support Services Help Desk is familiar with such features as keyboard access and other options important to people with disabilities.

Microsoft offers a teletypewriter (TTY) service for customers who are deaf or hard of hearing. For assistance in the United States, contact Microsoft Technical Support on a TTY at 1-800-892-5234. This service is available Monday through Friday 6:00 A.M. to 6:00 P.M. PST.

For information on additional support services, visit the Microsoft Accessibility Web site at http://www.microsoft.com/enable

8.3.5

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

AWS Response:

SHI’s content delivered through Web browsers is accessible through current released versions of Internet Explorer, Chrome, FireFox, and Safari.

CA Response:

CA SaaS applications are all delivered through the current releases of all major browsers, Internet Explorer, Chrome at a minimum.

Microsoft Response:

Azure supports several hardware platforms and browsers in order to perform tasks within the cloud platform. As Azure is computer based, using a mobile device or computer using a current browser is required.

The latest mobile devices are supported:

- All current mobile OS and one version back
- Blackberry OS (Excluding Blackberry Priv which operates on Android OS)

The latest versions of the following browsers are supported:

- Edge (latest)
- Internet Explorer (11 and up)
- Safari (7 and up)
- Chrome (latest)
- Firefox (latest)
- Safari 6 and lower are not supported. If you're using OS X, you can either use Chrome, Firefox, or upgrade to OS X Mavericks to get Safari 7.

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.

SHI Response:

SHI conducts one or more onboarding meetings with the Purchasing Entity and designees to define requirements and procedures needed for the purpose of account setup, provisioning of resources, access management, procurement and retirement of subcategory functionality offered under our IaaS and PaaS service models.

SHI does not require access to nor does it grant itself read, write, administrative or any other type of access to the subcategory resources used to store, process and transfer the data owned by the Purchasing Entity.

8.4 CUSTOMER SERVICE

8.4.1

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

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

SHI Response:

SHI provides a comprehensive customer support plan to ensure we are meeting each customer's needs. SHI's Account Executives are empowered to make decisions around the support of their customers, and they have the autonomy to resolve issues as they arise. Because our Account Executives are accountable and responsible for ensuring customer satisfaction, SHI is able to provide high quality customer service and ensure efficient and effective response to questions and issues. In addition, the SHI Regional Directors are engaged with the account teams to provide executive level support and to meet with customers as needed.

SHI believes in regular communication with our customers. SHI Account Executives meet with the Participating States and individual contract users to review their business with SHI. During these review meetings, we discuss purchase history, as well as the customer's future plans. With open discussions, SHI can provide tremendous value in supporting future initiatives and will engage the support teams as needed to meet the customer's goals and objectives.

SHI encourages and actively solicits customer feedback. Our Director of Quality collects customer comments and concerns to ensure they are addressed and resolved as quickly as possible. SHI sends an annual customer satisfaction survey to request feedback on our performance and the services we provide. By soliciting feedback, we remain in touch with our customers' needs.

SHI remains nimble in our approach to supporting our customers' IT needs, allowing us to address each customer on an individual basis. We understand that "one size does not fit all" and that philosophy is apparent in our service structure.

We believe our commitment to meeting our customers' needs is demonstrated in our level of success under the current NASPO ValuePoint SVAR agreement. SHI holds the most Participating Addenda and has achieved the most volume under the contract. We have met and exceeded service levels for NASPO ValuePoint and for each State during the contract term, and we have been an active participant in helping NASPO ValuePoint and the States to explore new avenues to achieve additional benefits under the contract.

Here is what one SHI customer has to say about SHI's ability to meet his organization's needs under the current SVAR contract:

"I am writing this letter to recommend SHI as a value added reseller of Software for the State of Arizona. I worked as an IT infrastructure manager for the Department of Corrections for six years and have been working at the City of Phoenix the past three years. I can attest that during my career in Information Technology I have never worked with a vendor that was more responsive and provided better customer service than SHI. When a quote was needed for software, SHI always provided timely service and never left us waiting. In addition SHI would contact and meet with our teams to make sure the needs of our organization were being met. When help was needed reconciling licensing SHI was accommodating and quick to help by providing useful reports. SHI is a great resource and truly an exceptional partner. I wholeheartedly recommend their services."

-John Ryan, City of Phoenix Information Technology Services

AWS Response:

- Quality assurance measures:
  - Average contacts to resolution
  - Average response time
- Escalation plan:
  - Dedicated resource escalates to SE immediately upon receipt of case, if requested by user, or if SLA is missed.
  - Support Engineer (SE) resource escalates to Sr. Support Engineer immediately upon receipt of case, if requested by user, or if second SLA is missed.
  - Sr. Support Engineer escalates to AWS engineering if SLA is missed.
  - Dedicated resource and highest Engineer resources is engaged on the case until completed and closed by the user.
- SLA = <12 hour response time

CA Response:

Metrics are developed and monitored independently within each business unit. These metrics and performance are reviewed during both our internal and external audits. High level metrics are reported and reviewed during the Management Reviews.

CA Technologies Quality Assurance:

CA’s SMART methodology for governance encompasses 2 Milestones: Build Commit and Go-to-Market Commit. These Milestones provide project level inspection to evaluate a projects plan and the execution of that plan before going to market. CA’s Agile@CA methodology for software development defines how CA designs, develops and tests software. Together, both SMART and Agile@CA provide a comprehensive framework for developing and delivering quality products.

QA processes are built into Agile@CA development process and with special emphasis within the Pre-Go to Market phase, which consists of develop, build, code, and test the product; for each build created, unit testing and build verification testing.

Customer validation of the product occurs as alpha/beta test cycles or earlier in the development with Agile end of sprint reviews. The validation plan is created as part of the pre-build commit activities and validated before completion of the Go to Market Commit.

Agile@CA process ensures QA involvement from the earliest start of the project. QA gains an understanding of the requirements. With a focus on Non-functional Requirements, testing such as performance and scalability are highlighted as elements for a testing plan.

The cross functional nature of the Agile Core Teams ensures that all aspects of the project are reviewed and ready to go to market.

QA develops detailed test cases based on the project test strategy and test coverage requirements. Test cases are reviewed with Development. Test automation is also completed where planned. Testing is executed in accordance with the QA Plan during Sprints or cycles. Defects are identified and triaged during these cycles. CA provides its teams with enterprise level test management, defect management, and test automation tools and practices to help assure high levels of quality.

Quality for CA PPM is achieved by a combination of manual, automation and performance testing. Since we practice Agile development process, we utilize continuous integration (CI) build approach that executes a battery of unit tests for every build to ascertain the health of the build. In addition, we continuously execute automated QA test cases twice a day (also called Continuous Regression Testing (CRT) on a passed CI build. We use a combination of JUnit, Testing, Selenium and home-grown testing tools to subject our application to 5000+ automated test cases and scripts. Performance testing is done using Load Runner and SilkPerformer periodically. We perform various configuration testing with application deployed on architectural stack supported by CA PPM. Data-scrubbed versions of customer dataset are used to perform upgrade and end to end customer scenario testing. QA test cases are manually executed on fresh install and QA dataset upgrade as well.

Customer validation of the product occurs as alpha/beta test cycles or earlier in the development with Agile end of sprint reviews. The validation plan is created as part of the pre-build commit activities and validated before completion of the Go to Market Commit.

Customers can escalate any issue within the system. In addition, if incident resolution objectives are not met, CA Technologies follows a defined escalation process. Escalations are assessed by the CA Support management team and are assigned to escalation manager that “owns” the escalation to resolution. The escalation manager will provide regular updates to the customer and CA Technologies management so that appropriate CA Technologies resources are brought into the resolution effort. The escalation manager will also be the central point of contact for the customer until the escalation is considered resolved.

CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly.

Microsoft Response:

For complete details regarding Microsoft product SLAs, visit www.microsoftvolumelicensing.com

Azure Active Directory

We guarantee at least 99.9% availability of the Azure Active Directory Basic and Premium services. The services are considered available in the following scenarios:

- Users are able to login to the service, login to the Access Panel, access applications on the Access Panel and reset passwords.
- IT administrators are able to create, read, write and delete entries in the directory or provision or de-provision users to applications in the directory.

No SLA is provided for the Free tier of Azure Active Directory.

API Management

- We guarantee that API Management Service instances running in the Standard tier will respond to requests to perform operations at least 99.9% of the time.
- We guarantee that API Management Service instances running in the Premium tier deployed across two or more regions will respond to requests to perform operations at least 99.95% of the time.

No SLA is provided for the Developer tier of the API Management Service.

View full details

App Service

We guarantee that Web Apps running in a customer subscription will be available 99.95% of the time. No SLA is provided for Mobile Apps, Logic Apps, or API Apps while such services are still in Preview or for Apps under either the Free or Shared tiers.

Application Gateway

We guarantee that each Application Gateway Cloud Service having two or more medium or larger instances will be available at least 99.9% of the time.

Automation

We guarantee that at least 99.9% of runbook jobs will start within 30 minutes of their planned start times.

We guarantee at least 99.9% availability of the Azure Automation DSC agent service.

No SLA is provided for the Free tier of Azure Automation.

Backup

We guarantee at least 99.9% availability of the backup and restore functionality of the Azure Backup service.

BizTalk Services

We guarantee that at least 99.9% of the time customers will have connectivity between their BizTalk Service Environments in the Basic, Standard and Premium tiers and our Internet gateway. We do not offer an SLA for the BizTalk Services Developer tier.

Cache

We guarantee at least 99.9% of the time that customers will have connectivity between the Cache endpoints and our Internet gateway.

CDN

We guarantee that at least 99.9% of the time CDN will respond to client requests and deliver the requested content without error. We will review and accept data from any commercially reasonable independent measurement system that you choose to monitor your content. You must select a set of agents from the measurement system's list of standard agents that are generally available and represent at least five geographically diverse locations in major worldwide metropolitan areas (excluding PR of China).

Cloud Services and Virtual Machines

- For Cloud Services, we guarantee that when you deploy two or more role instances in different fault and upgrade domains, your Internet facing roles will have external connectivity at least 99.95% of the time.
- For all Internet facing Virtual Machines that have two or more instances deployed in the same Availability Set, we guarantee you will have external connectivity at least 99.95% of the time.

DocumentDB

We guarantee at least 99.95% of the time we will successfully process requests to perform operations against DocumentDB Resources.

ExpressRoute

We guarantee a minimum of 99.9% ExpressRoute dedicated circuit availability.

HDInsight

For HDInsight, we guarantee that any HDInsight Cluster that you deploy will have external connectivity at least 99.9% of the time over a monthly billing cycle.

IoT Hub

- For IoT Hub, we promise that at least 99.9% of the time deployed IoT hubs will be able to send messages to and receive messages from registered devices and the Service will able to perform create, read, update, and delete operations on IoT hubs.
- No SLA is provided for the Free Tier of IoT Hub.

Key Vault

We guarantee that we will process Key Vault transactions within 5 seconds at least 99.9% of the time.

Machine Learning

- For the Request Response Service (RRS), we guarantee 99.95% availability of API transactions.
- For the Batch Execution Service (BES) and management APIs, we guarantee 99.9% availability of API transactions.

No SLA is provided for the free tier of Machine Learning.

Media Services

- For Media Services Encoding, we guarantee 99.9% availability of REST API transactions.
- For Streaming, we will successfully service requests with a 99.9% availability guarantee for existing media content when at least one Streaming Unit is purchased.
- For Live Channels, we guarantee that running Channels will have external connectivity at least 99.9% of the time.
- For Content Protection, we guarantee that we will successfully fulfill key requests at least 99.9% of the time.
- For Indexer, we will successfully service Indexer Task requests processed with an Encoding Reserved Unit 99.9% of the time.

Mobile Engagement

We guarantee at least 99.9% availability of REST API calls to the Azure Mobile Engagement Service. No SLA is provided for the free tier.

Mobile Services

We guarantee 99.9% availability of REST API calls to all provisioned Azure Mobile Services running in Standard and Premium tiers in a customer subscription. No SLA is provided for the free tier of Mobile Services.

Multi-Factor Authentication

We guarantee 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process authentication requests for the Multi-Factor authentication provider deployed in a customer subscription.

Operational Insights

We guarantee that at least 99.9% of the time, log data will be indexed within six hours of the data being queued for indexing by the Operational Insights Service.

No SLA is provided for the free tier of Azure Operational Insights.

RemoteApp

We guarantee at least 99.9% of the time users will have connectivity to their applications through the RemoteApp service. No SLA is provided for the free tier of RemoteApp.

Scheduler

We guarantee that at least 99.9% of the time all scheduled jobs will initiate within 30 minutes of their planned execution times.

Search

We guarantee at least 99.9% availability for index query requests when an Azure Search Service Instance is configured with two or more replicas, and index update requests when an Azure Search Service Instance is configured with three or more replicas. No SLA is provided for the free tier.

Service Bus

- For Service Bus Relays, we guarantee that at least 99.9% of the time, properly configured applications will be able to establish a connection to a deployed Relay.
- For Service Bus Queues and Topics, we guarantee that at least 99.9% of the time, properly configured applications will be able to send or receive messages or perform other operations on a deployed Queue or Topic.
- For Service Bus Basic and Standard Notification Hub tiers, we guarantee that at least 99.9% of the time, properly configured applications will be able to send notifications or perform registration management operations with respect to a Notification Hub.
- For Event Hubs Basic and Standard tiers, we guarantee that at least 99.9% of the time, properly configured applications will be able to send or receive messages or perform other operations on the Event Hub.

Site Recovery

- For each Protected Instance configured for On-Premises-to-On-Premises Failover, we guarantee at least 99.9% availability of the Site Recovery service.
- For each Protected Instance configured for On-Premises-to-Azure planned and unplanned Failover, we guarantee a four-hour Recovery Time Objective for unencrypted Protected Instances, and a six-hour Recovery Time Objective for encrypted Protected Instance, depending on the size of the Protected Instance.

SQL Database

Web and Business Tiers

We guarantee at least 99.9% of the time customers will have connectivity between their Web or Business Microsoft Azure SQL Database and our Internet gateway.

Basic, Standard, and Premium Tiers

We guarantee at least 99.99% of the time customers will have connectivity between their Basic, Standard, or Premium Microsoft Azure SQL Database and our Internet gateway.

Storage

- We guarantee that at least 99.99% of the time, we will successfully process requests to read data from Read Access-Geo Redundant Storage (RA-GRS) Accounts, provided that failed attempts to read data from the primary region are retried on the secondary region.
- We guarantee that at least 99.9% of the time, we will successfully process requests to read data from Locally Redundant Storage (LRS), Zone Redundant Storage (ZRS), and Geo Redundant Storage (GRS) Accounts.
- We guarantee that at least 99.9% of the time, we will successfully process requests to write data to Locally Redundant Storage (LRS), Zone Redundant Storage (ZRS), and Geo Redundant Storage (GRS) Accounts and Read Access-Geo Redundant Storage (RA-GRS) Accounts.

StorSimple

We guarantee at least 99.9% availability of the backup, cloud tiering, and restore functionality of the Azure StorSimple service.

Stream Analytics

- We guarantee at least 99.9% availability of the Stream Analytics API.
- We guarantee that 99.9% of the time, deployed Stream Analytics jobs will be either processing data or available to process data.

Traffic Manager

We guarantee that DNS queries will receive a valid response from at least one of our Azure Traffic Manager name server clusters at least 99.99% of the time.

Visual Studio Team Services

- We guarantee at least 99.9% availability of Visual Studio Team Services for paid Visual Studio Team Services users to access the associated Visual Studio Team Services account.
- We guarantee at least 99.9% availability to execute build operations using the paid Visual Studio Team Services Build Service.
- We guarantee at least 99.9% availability to execute load testing operations using the paid Visual Studio Team Services Load Testing Service.
- We guarantee at least 99.9% availability to execute build and deployment operations using the paid Visual Studio Team Services Build & Deployment Service.

VPN Gateway

We guarantee 99.9% availability for each VPN Gateway.

Microsoft will provide at least 90 days' notice for adverse material changes to any of the SLAs listed above.

Availability for all Azure services is calculated over a monthly billing cycle.

Incidents can be reported through the Azure Management Portal as well. Security incidents are provided through the Azure Management portal in addition to being placed on the Azure Health Dashboard.

Azure Support options are available as an additional cost.

- Free: No phone support
- Developer: No phone support. Email or Instant Messaging Support only
- Standard: 3 support calls per month
- Professional Direct: Unlimited support calls per month per and escalation line
- Premier: Unlimited support calls per month per an escalation line and onsite services

8.4.2

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

- *You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.*
- *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.*
- *Customer Service Representative will respond to inquiries within one business day.*
- *You must provide design services for the applicable categories.*
- *You must provide Installation Services for the applicable categories.*

SHI Response:

At SHI, our people remain our greatest asset. All members of the SHI Account Team are dedicated to providing high quality customer service and support. Our success has stemmed from outstanding customer support through dedicated Account Teams, constant development of procurement and Internet solutions, strong partnerships with top manufacturers, and a company-wide determination to be the best.

SHI has 88 Public Sector dedicated, field based Account Executives across the country today. We continue to expand our footprint rapidly.

SHI can comply with the requirement of having a lead representative for Participating Entity. We are happy to publish a current list contact information for our Account Executive team on a regular basis to NASPO.

SHI has representative's available Monday through Friday from 7-6AM to support our customers. As needed SHI will adjust hours to respond to emergencies or other high priority needs.

SHI has an SLA of 4 hours from inquiry and then our team will follow up with 24 hours or as needed until the request is completed.

The dedicated SHI Account Team will help the Participating Entity contact our cloud partners for scoping and services surrounding all of our partners. SHI will work jointly with our partners to provide Design Services for all categories as well Installation Services for all categories.

Specifically for AWS solutions, SHI currently provides:

- <12 hour response SLA
- 8am-7pm ET
- Mon-Fri
- Design Services
- Installation Services are available as part of defined statement of work (SOW)

Upon award a dedicated resource responsible for emergency notifications and weekend coverage will be provided.

CA Response:

A service delivery manager will be assigned to each SaaS subscriber. CA provides 24x7x365 support for Severity 1 cases. All severity 1 cases must be submitted via telephone. Access to CA Support Online is available 24x7x365 for online technical support and access to CA software product and documentation downloads, fixes, service packs, patch downloads, communities, beta testing, FAQs, samples, webcast recordings and demos, usage tips, technical updates and HYPER notifications, as such are made available by CA. CA will use reasonable efforts to meet the service level objectives stated below with regard to remedial software support and will provide ongoing efforts to resolve Severity 1 support cases. All cases can be submitted to CA on a 24 hours per day, 7 days per week, 365 days per year basis. Due to the complexities of technical environments, the model represents an estimate of response times only and actual response times may vary.

Response Level Objectives:

- 1 hour for Severity 1 cases (24x7)
- 2 business hours for Severity 2 cases (During normal business hours, as published on CA Support Online, based on the time a case is initially submitted online or telephonically.)
- 4 business hours for Severity 3 cases (During normal business hours, as published on CA Support Online, based on the time a case is initially submitted online or telephonically.)
- 1 business day for Severity 4 cases (During normal business hours, as published on CA Support Online, based on the time a case is initially submitted online or telephonically.)

CA Services are available for configuration and design of the service. No installation is necessary to consume the stock service.

Microsoft Response:

Phone Support will be offered on a 24/7 basis

There are five levels of support available:

- Free: No supported email or phone support available. However there are forums headed by Microsoft MVP associates and employees.
- Developer: 8 hour response time
- Standard: 2 hour response time
- Professional Direct: 1 hour response time
- Premier: 15 minute response time

8.5 SECURITY OF INFORMATION

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

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.

AWS Response:

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

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

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

Data Recovery/Transfer

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

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

Deleting Data

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

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

Archiving Data

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

AWS Storage Device Decommissioning

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

CA Response:

CA Technologies has a comprehensive Data Protection Program in place which is designed to respect the privacy of its employees, customers, vendors, partners and all third parties with whom CA Technologies interacts. CA Technologies is committed to complying with all applicable laws relating to privacy and data protection worldwide. As part of CA Technologies' efforts in this area, it has certified to the US-EU and US-Swiss Safe Harbor Frameworks and applies those principles on a worldwide basis. Employees are made aware of their obligations with respect to privacy by means of corporate policy and procedure, employee communications and training. CA Technologies has privacy officers who address data protection issues that arise in their respective geographies. CA Technologies external privacy notice describes how CA Technologies handles personal information and it can be found at www.ca.com/us/privacy.

Microsoft Response:

Microsoft datacenters receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified. Microsoft datacenters are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. Datacenters are surrounded by a fence with access restricted through badge controlled gates.

Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities.

CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.

Data destruction techniques vary depending on the type of data object being destroyed, whether it be subscriptions, storage, virtual machines, or databases. In Azure's multi-tenant environment, careful attention is taken to ensure that one customer's data is not allowed to either "leak" into another customer's data, or when a customer deletes data, no other customer (including, in most cases, the customer who once owned the data) can gain access to that deleted data.

Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.

8.5.2

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

SHI Response:

SHI does not have access to any stored, processed or transferred data running in the IaaS and/or PaaS services and subcategory functionality.

AWS Response:

AWS does not access any stored, processed of transferred data running in its IaaS and/or PaaS services unless expressly as described in it Terms of Use.

CA Response:

See response to 8.5.1

Microsoft Response:

Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Azure asset owners are responsible for maintaining up-to-date information regarding their assets.

Microsoft datacenters receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified. Microsoft datacenters are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. Datacenters are surrounded by a fence with access restricted through badge controlled gates.

Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities.

CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.

MCIO, and consequently Azure, maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. MCIO turns off unused ports by default to prevent unauthorized access.

Microsoft Azure Fabric Controlled Hardware Device Authentication maintains a set of credentials (keys and/or passwords) used to authenticate itself to various Microsoft Azure hardware devices under its control. The system used for transporting, persisting, and using these credentials is designed to make it unnecessary for Microsoft Azure developers, administrators, and backup services/personnel to be exposed to secret information.

Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored while using Azure services such as Site Recovery and Backup.

Data destruction techniques vary depending on the type of data object being destroyed, whether it be subscriptions, storage, virtual machines, or databases. In Azure's multi-tenant environment, careful attention is taken to ensure that one customer’s data is not allowed to either “leak” into another customer’s data, or when a customer deletes data, no other customer (including, in most cases, the customer who once owned the data) can gain access to that deleted data.

Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.

Microsoft Information Security policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited.

Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests are required to wear guest badges and be escorted by authorized Microsoft personnel.

Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.

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.

AWS Response:

We will not have any access to a Purchasing Entity's data because it does not need such access to deliver IaaS and PaaS services, and because it cannot grant itself such access to the users' resources.

CA Response:

See response to 8.5.1

Microsoft Response:

Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as you direct, (2) with permission from an end user, (3) as described here or in your agreement(s), or (4) as required by law.

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

Upon receipt of any other third party request for Customer Data (such as requests from customer's end users), Microsoft will promptly notify you unless prohibited by law. If Microsoft is not required by law to disclose the Customer Data, Microsoft will reject the request. If the request is valid and Microsoft could be compelled to disclose the requested information, Microsoft will attempt to redirect the third party to request the Customer Data from you.

Except as customer directs, Microsoft will not provide any third party: (1) direct, indirect, blanket or unfettered access to Customer Data; (2) the platform encryption keys used to secure Customer Data or the ability to break such encryption; or (3) any kind of access to Customer Data if Microsoft is aware that such data is used for purposes other than those stated in the request.

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

We will not disclose Administrator Data, Payment Data or Support Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as you direct, (2) with permission from an end user, (3) as described here or in your agreement(s), or (4) as required by law. We may share Administrator Data or Payment Data with third parties for purposes of fraud prevention or to process payment transactions.

The Online Services may enable you to purchase, subscribe to, or use services, software, and content from companies other than Microsoft ("Third Party Offerings"). If you choose to purchase, subscribe to, or use a Third Party Offering, we may provide the third party with your Administrator Data or Payment Data. Subject to your contact preferences, the third party may use your Administrator Data to send you promotional communications. Use of that information and your use of a Third Party Offering will be governed by the third party's privacy statement and policies.

8.6 PRIVACY AND SECURITY

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

8.6.1

Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

AWS Response:

The AWS solution does not require and does not accept access to any Procurement Entity users' data in order to provide IaaS and PaaS services and subcategory service functionality. Users are entirely able to retain full responsibility for encrypting, safeguarding and appropriately handling their Low, Moderate and High Risk data in compliance with any oversight guidelines.

The offered IaaS and PaaS services are audited and certified to meet the needs of various data handling standards as listed in section 8.6.2.

CA Response:

CA Technologies understands that security is a top concern when evaluating cloud-based applications, which is why CA technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis. We use CIS and NIST standards as baselines for hardening our systems. We are currently working towards a NIST 800-53r4 certification however this is not yet complete. We are continuously reviewing our compliance with these standards. We perform monthly scans against our Production Infrastructure based on CIS standards. We scan for both vulnerabilities and compliance best practices bases on NIST 800-53v4 standards. Vulnerabilities are tracked and remediated based on severity and risk.

Microsoft Response:

Both Azure and the underlying Microsoft Cloud and Infrastructure Operations (MCIO) physical environments employ security frameworks that span multiple standards, including the ISO 27000 family of standards, NIST 800, and others. Please see Microsoft Azure CCM document for additional

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 Response:

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

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

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

CA Response:

Agile - Our data center provider has a SOC 2 audit report that can be provided upon request. Our application does not currently have such certifications.

APIM - The datacenters used by CA Technologies annually undergo SOC 3 audits. A copy of the latest SOC 3 report can be found here: http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

ASM - Rackspace datacenters annually undergo various certification including SOC 3 audits. All certifications are listed here: https://www.rackspace.com/en-us/security/management

The application currently does not hold a SOC 2 certification.

MAA - CA MAA is certified for SOC 2 Type 1 Security Audit.

PPM - SSAE-16 Type II SOC 2 and Soc 1; FedRAMP – (in progress for 2016)

8.6.3

Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

AWS Response:

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

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

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

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

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

- **Distributed Denial Of Service (DDoS) Attacks.** AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.
- **IP Spoofing.** Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

- **Port Scanning**. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by you. Your strict management of security groups can further mitigate the threat of port scans. If you configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, you must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

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

CA Response:

Agile/APIM - CA Technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. We also contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis. We use a co-located data center provider and within that environment we have a dedicated cage to which only our Operations Team has access. We also monitor all traffic across our systems using HIDS (OSSEC) and NIDS (Snort) to notify of any suspicious activity. As a SaaS application it can be accesses anywhere in the world. Customers have the ability to implement subscription level IP restrictions for restricting access to their subscription.

ASM - All ASM core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The ASM dashboard and API are protected with HTTPS/TLS encryption, and users are required to use a username and password to login to their accounts.

MAA - All MAA core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The MAA dashboard and API are protected with HTTPS/TLS encryption, and users are required to authenticate in order to access these.

PPM - CA Technologies contracts with an independent, third party vendor to evaluate and validate the security of our service on an ongoing basis. Critical and high risks are identified, validated, and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis. Ongoing scans are performed to ensure that no new risks have been introduced. Two types of scans are performed:

- Vulnerability Scans: Vulnerability tests are performed weekly
- Penetration Scans: Penetration tests are performed as each new release of the Service is being made available and no less than annually

Microsoft Response:

In addition to the information below, please see the response to question 8.5.2.

Azure Employees and contractors must have a business need to enter a Microsoft datacenter and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis. Failure to abide by the Microsoft Datacenter security policies means instant dismissal for the employee.

Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized Microsoft personnel.

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).

AWS Response:

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

CA Response:

Agile/APIM - All customer data is treated as confidential and as a policy we do not access customer data without explicit written consent. Access to systems containing customer data is restricted to our Operations Team according to our Elevated Permissions Policy. All personnel with access to client data undergo annual, mandatory security training and are covered under the CA Technologies NDA. Violations of security policies are grounds for termination. All access to data and other resources used to deliver the service are granted under the least principle.

ASM - Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to ASM servers, and database administrators have access to database servers. Account access is reviewed periodically. All data on CA laptops are encrypted and a PIN is required to boot.

MAA - Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to MAA servers, and database administrators have access to database servers. Account access is reviewed periodically.

PPM - All personnel with access to client data undergo annual, mandatory security training and are covered under the CA Technologies NDA. Violations of security policies are grounds for termination. All access to data and other resources used to deliver the service are granted under the least principle.

Microsoft Response:

Please see response to 8.5.3

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.

AWS Response:

Please see the response to question 8.6.2

CA Response:

Please see the response to question 8.6.2

Microsoft Response:

Please see the response to question 8.6.2. Additional information can also be found in the Microsoft Azure CCM document and online at the Azure Trust Center

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.

AWS Response:

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

AWS CloudTrail

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

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

- For information on the services and features supported by AWS CloudTrail, visit the AWS CloudTrail FAQs on the AWS website.
- The AWS whitepaper *Security at Scale: Logging In AWS* provides an overview of common compliance requirements related to logging, detailing how AWS CloudTrail features can help satisfy these requirements.
- The AWS whitepaper *Auditing Security Checklist for Use of AWS* provides customers with a checklist to assist in evaluating AWS for the purposes of an internal review or external audit.

AWS CloudTrail Features and Benefits

Some of the many features of AWS CloudTrail include:

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

Amazon CloudWatch

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

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

LogAnalyzer for Amazon CloudFront

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

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

Reports Generated

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

Third Party Tools

Many third-party log monitoring and analysis tools are available on AWS Marketplace.

AWS Identity and Access Management (IAM):

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

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

CA Response:

Agile and APIM - CA has various log monitoring tools that help us keep track of live production systems in order to understand load vs. resource utilization vs. performance. CA along with AWS monitors the service and provides real time alerting when systems suddenly die, or when system loads or response times approach critical thresholds. Logs are kept for forensic examination and identification of trends in order to proactively ensure stability. All systems are required to send logs to a centralized log server. At a minimum log data must contain timestamps, usernames, IP Addresses, and query parameters.

ASM - ASM servers log all activity, and data retention is anywhere from 30 days to 1 year depending on the application and volume of logs generated.

MAA - CA MAA servers log all activity, and data retention is anywhere from 14 to 180 days depending on the component and volume of logs generated.

PPM - systems are monitored 24 x 7 by an enterprise network intrusion protection solution. Audit logs are sent to a centralized CA Audit system and are reviewed daily to ensure that there is no unusual activity.

Microsoft Response:

Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on secure infrastructure and are retained for 180 days.

Microsoft Identity Manager and intrusion detection system tools are implemented within the Azure environment. Azure uses an early warning system to support real-time analysis of security events within its operational environment. Monitoring agents and the alert and incident management system generate near real-time alerts about events that could potentially compromise the system.

MCIO has established procedures to receive, generate and disseminate security alerts from external organizations as necessary. MCIO coordinates with external agencies regarding the implementing of security directives.

The Azure logging and monitoring infrastructure encompasses the entire Azure platform and does not vary by tenant. Detected incidents are isolated or contained in the most effective way depending on the nature of the event.

The Azure platform is specifically designed and architected to prevent the possibility of production data being moved or replicated outside of the Azure cloud environment. These controls include:

- Physical and logical network boundaries with strictly enforced change control policies
- Segregation of duties requiring a business need to access an environment
- Highly restricted physical and logical access to the cloud environment

- Strict controls based on SDL and OSA that define coding practices, quality testing and code promotion
- Ongoing security, privacy and secure coding practices awareness and training
- Continuous logging and audit of system access
- Regular compliance audits to ensure control effectiveness

Microsoft Azure customers are responsible for defining policies and establishing controls for how their production data is maintained with regard to replication or high-availability and the demarcation of their production environment.

Azure Employees and contractors must have a business need to enter a Microsoft datacenter and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis. Failure to abide by the Microsoft Datacenter security policies means instant dismissal for the employee.

Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Microsoft Azure platform components (including OS, Virtual Network, Fabric, etc.) are configured to log and collect security events.

Microsoft Azure uses Active Directory (AD) to manage and provision user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity.

Strong authentication, including the use of multi-factor authentication, helps limit access to customer data to authorized personnel only. Sample audits are performed by both Microsoft and third parties to attest that access is only for appropriate business purposes. When access is granted, it is carefully controlled and logged, and revoked as soon as it is no longer needed.

The operational processes and controls that govern access and use of customer data in Azure are rigorously maintained and regularly verified by accredited audit firms.

Designated security group owners within Microsoft Azure are responsible for reviewing appropriateness of employee access to applications and data on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has taken place. Access is modified based on the results of this review.

Membership in security groups must be approved by security group owners. Automated procedures are in place to disable AD accounts upon the user's leave-date.

Physical access to infrastructure systems is restricted to Microsoft operations personnel or designated and authorized third-party contractors at datacenter locations. Access is logged and reviewed by security managers.

Within the Microsoft Azure environment, customers are responsible for managing access to the applications customers host on Microsoft Azure.

8.6.7

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

AWS Response:

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

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

CA Response:

Agile - Our databases are shared but logically segregated. We ensure logical security of access to customer data by implementing access restrictions between subscriptions and roles within those subscriptions to assure adequate segregation of data. There is a plugin available in the unlimited edition that allows the administrator to limit access to the application based on IP address.

APIM – Users of the Portal are divided into two types: Internal users (for publishers of the API) and External users (for developers). There are a number of pre-defined roles for both Internal and External users that inherit functionality in a hierarchical manner. Portal has RBAC built in that allows you to grant access to different functionality for different users. For example, you can assign a user to role that only allows them access to update content, or access apps but not create them.

ASM – Only Public Status Page (PSP) data is stored in the cloud, and PSP web pages are accessible by anyone. PSP data is only sent to the cloud if the customer enables this feature, and they can decide which data is made public.

MAA – CA utilizes IaaS vendor to host the service with strict access controls in place. CA SaaS InfoSec team manages users and their associations with groups within LDAP Directory and conducts periodic access reviews to conform to governance requirements.

PPM – Within the CA PPM SaaS application, over 150 individual rights/roles/groups can be used to secure application functionality and data records. Additionally, standard audit trail functionality can be configured for most objects and attributes to capture creation, edits, and deletions of selected data records or attributes.

Microsoft Response:

Visibility for Azure can be restricted through the use of Role Based Access Controls. This feature can limit what users have access into and functionality.

8.6.8

Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

AWS Response:

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

CA Response:

CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant parties for notification. All security incidents will be investigated and triaged to understand where the vulnerability exists. Software vulnerabilities will be investigated by CA engineering teams; other vulnerabilities will be addressed by the SaaS Ops team in conjunction with AWS. Affected customers will be notified and given a remediation plan. Clients are notified via email of any security incident that resulted in a data breach for that client promptly and no later than 5 days. A root cause analysis is then sent within 30 days. A meeting to review and discuss can be setup upon request.

Microsoft Response:

Microsoft Azure Incident Severity Table

Microsoft Azure Broad Commercial Cloud Support Incidents

Severity	Customer's situation	Expected Microsoft Response	Expected Customer Response
A	Critical business impact: • Customer's business has significant loss or degradation of services • Needs immediate attention	• Initial response: o 1 hour or less for Professional Direct o 2 hours or less for Standard	• Allocation of appropriate resources to sustain continuous effort all day, every day • Accurate contact information on case owner

	Severity A support is only available for the *Microsoft Azure Standard and the Microsoft Azure Professional Direct* support offerings. If you are a Premier customer, please login to your Premier portal to submit your issue.	• Continuous effort all day, every day	
B	Moderate business impact: • Customer’s business has moderate loss or degradation of services but work can reasonably continue in an impaired manner. • Needs attention within 2 business hours (review note 1)	• Initial response: o 2 hours or less for Professional Direct o 4 hours or less for Standard • 24x7 continuous effort unless customer requests to opt-out	• Allocation of appropriate resources to sustain continuous effort unless customer requests to opt-out of 24x7 • Accurate contact information on case owner
C	Minimum business impact: • Customer’s business is substantially functioning with minor or no impediments of services. • Needs attention within 4 business hours (review note 1)	• Initial response: o 4 hours or less for Professional Direct o 8 hours or less for Standard o Developer (business hours only; 8 hours or less	• Accurate contact information on case owner

1. Business Hours are defined as 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday excluding holidays for North America. Local hours of operation and business hours can be found at http://support.microsoft.com/contactus.

Microsoft may downgrade the severity level if the customer is not able to provide adequate resources or responses to enable Microsoft to continue with problem resolution efforts.

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.

AWS Response:

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

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

CA Response:

Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.

The datacenters used by CA Technologies annually undergo SOC 3 audits. A copy of the latest SOC 3 report can be found here:
http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

Microsoft Response:

Azure has several datacenters in the United States and abroad. The security controls of said datacenters are detailed in the Microsoft Azure CCM document.

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)

AWS Response:

The following whitepapers may prove helpful in your formulation of a response to these questions.

Architecting for the Cloud AWS Best Practices Feb 2016

https://aws.amazon.com/whitepapers/architecting-for-the-aws-cloud-best-practices/

Managing Your AWS Infrastructure at Scale Feb 2015

https://d0.awsstatic.com/whitepapers/managing-your-aws-infrastructure-at-scale.pdf

CA Response:

Only SaaS is provided, network diagram can be provided upon signing NDA.

Microsoft Response:

Please see the response for question 6.7 for details.

8.7 MIGRATION AND REDEPLOYMENT PLAN

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

SHI will work closely with our customers and partners in the event that end of life activities take place. We can help to create a plan to deprovision data/services ahead of time and offer project management around the migration to whatever solution the customer has chosen.

8.7.1

Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

AWS Response:

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

CA Response:

Agile, APIM, ASM - The customer is responsible for the lifecycle of their data. We will retain and protect all data until it has been deleted from our systems. We can remove data from our systems upon written request from the customer at termination of the contract.

MAA - Tenant deprovisioning procedures are followed when customers decide to discontinue the service. As part of deprovisioning, any footprints of tenant's configurations and data is decommissioned.

PPM - Upon termination of the service a client's PPM SaaS instance is deprovisioned and all client data is programmatically deleted per the stated data retention policies. Data can be delivered per the response in 8.7.2. All security measures remain in place during this phase. The client retains ownership of all data contained in the service both during the term of contract and after it expires

Microsoft Response:

Any service can be deleted via PowerShell or the Azure Management Portal. Any data created via the deleted service will be contained in Azure Storage unless this was deleted along with the service. Any created security policies within the storage container will be maintained. All necessary SLA’s are covered in 8.10.2.

8.7.2

Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

AWS Response:

SHI will work with the Purchasing Entity to prevent any disruption and suspension in IaaS or PaaS services. If a suspension or retrieval effort is required, SHI will petition AWS and will work in good faith to accommodate expedient reinstatement of services, transfer of services and data, or any combination thereof to prevent data stranding.

CA Response:

All Terminating clients have the option to receive their data, this option will be discussed during termination process. We can provide an export of the data in XML and JSON formats at the end of the contract.

For ASM, this solution is currently not available, due to nature of offering. All request will be handled on a case by case basis.

MAA – This solution is currently not available.

PPM - Terminating clients have the following options to receive their data:

- API data extractions via HTTPS producing XML formatted flat files. See the user guide XOG Developer Guide for technical details.
- Oracle data pump generated file containing all tables with client data.
- Oracle data pump generated file of the client's entire CA PPM database schema. This option requires a valid, perpetual CA PPM license.

Microsoft Response:

Please see our response to question 8.11.

8.8 SERVICE OR DATA RECOVERY

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

8.8.1

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

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

AWS Response:

Our combined view, SHI and AWS, is that the best way to address downtime and data recovery scenarios is to design redundancy and resiliency from the very start. The AWS platform provides the necessary services, subcategories, and functionality needed to design and build high resilience environments:

- Extended downtime and System failure – provision standby storage and compute resources, in applicable legal and geographic jurisdictions, so that outages are quickly averted by powering-up these standby resources. Provide appropriate user designees' the access and ability to power-up these standby resources without needing any external assistance.

- Loss of data – secure data in redundant locations in compliance with applicable legal and regulatory requirements.   Enable full use of AWS' eleven-nines of data durability in each region and availability zone to prevent loss.

Recovery objectives, and RPO and RTO goals – help users classify and clarify required recovery objectives and applicable RPO/RTO goals, then offer designs suited to support availability requirements, support ongoing audits to ensure goals are consistently met.

CA Response:

For Agile and APIM - Disaster to the CA Technologies corporate network in New York will not affect customers' service. Secondary services, such as domain name services will be routed through the secondary CA Technologies network in Illinois. CA has a BCP plan in place to direct its services. The SaaS environment is separate from the CA corporate network and a service specific disaster recovery plan is in place.

In the event of downtime we would failover to our warm data center in order to restore access to the application as quickly as possible. This is done according to our Disaster Recovery Plan. We have implemented a physical standby database in both hot/Live site as well as warm/standby sites using Oracle Data Guard with real-time apply to achieve the stated recovery objectives. We enable all of our employees with the ability to be able to work remotely and provide remote network access to ensure business functions can continue. All corporate infrastructure has redundant systems that can be utilized in the event of failure.

CA provides an SLA of 99.8% uptime, which can result in unforeseen outages of ~1.5 hours per month. In the event of a failure to meet a SLA threshold, customer may be entitled to a number of days of credit.

Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs.

Recovery Point Objective (RPO): Maximum data loss: 24 hours
Data that is uploaded, but not backed up within the 24 hours may have to be re-entered
Recovery Time Objective (RTO): 72 hours

ASM - If unable to resolve in a timely manner, all customers will be notified via email to the registered admin. Failover from the primary to DR site may be utilized if the extended amount of time warrants declaration of DR. Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs. Customers would be notified in advance, and given ample time to retrieve their data manually or via the ASM API. Data is replicated from the primary (production) to secondary (DR) continuously. In the event of catastrophic loss of live data a failover to the DR site would be necessary.

Recovery Point Objective (RPO): Maximum data loss: 24 hours
Data that is uploaded, but not backed up within the 24 hours may have to be re-entered
Recovery Time Objective (RTO): 24 hours

MAA – Customers are kept abreast with progress during incidents, including outages. CA utilizes best-of-breed notification system which enables customer contacts to self-subscribe to different types of notifications that they would be interested in. A DR plan has been created should the extended down time result in DR declaration. MAA data is backed up fully daily. The maximum data loss would be the previous 24hrs. Customers would be notified in advance, and given ample time to retrieve their data. Using DB clustering technologies, multiple copies of data are maintained helping in recovery of the data.

Recovery Point Objective (RPO): Maximum data loss: 24 hours
Data that is uploaded, but not backed up within the 24 hours may have to be re-entered
Recovery Time Objective (RTO): 72 hours

PPM - Hardware/software failure: Because of high availability and redundancy there should be zero loss of data in this scenario, but in rare cases, data may be lost up to the last available recovery point. CA Technologies will use all commercially reasonable efforts to recover from any system failure event as follows:

Recovery Point Objective: 24 hours or less
Recovery Time Objective: 4 hours

Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs. Disaster to the CA Technologies corporate network in New York will not affect customers' service. Secondary services, such as domain name services will be routed through the secondary CA Technologies network in Illinois.

Recovery Point Objective (RPO): Maximum data loss: 24 hours
Data that is uploaded, but not backed up within the 24 hours may have to be re-entered
Recovery Time Objective (RTO): 72 hours

Microsoft Response:

BCPs have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.

The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.

8.8.2

Describe your methodologies for the following backup and restore services:

- *Method of data backups*
- *Method of server image backups*
- *Digital location of backup storage (secondary storage, tape, etc.)*
- *Alternate data center strategies for primary data centers within the continental United States.*

AWS Response:

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

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

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

Protecting Configurations Rather Than Servers

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

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

A sample workflow is as follows:

- Launch a new instance of a web server, passing it the identity of the web server and any security credentials required for initial setup. The instance is based upon a pre-built AMI that contains the operating system and relevant web server application (e.g., Apache or IIS).
- Upon startup, a boot script accesses a designated and secured Amazon Simple Storage Service (Amazon S3) bucket that contains the specified configuration file(s).
- The configuration file contains various instructions for setting up the server (e.g., web server parameters, locations of related servers, additional software to install, and patch updates).
- The server executes the specified configuration and is ready for service. An open-source tool for performing this process called cloud-init is already installed on Amazon Linux AMIs and is also available for a number of other Linux distributions.

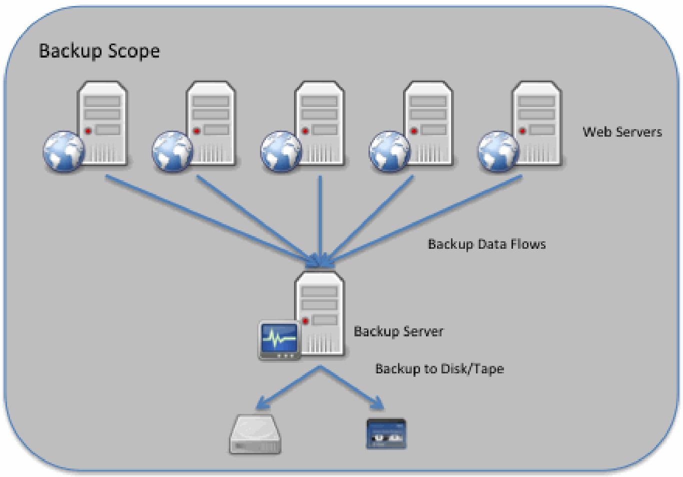


Figure – Traditional Backup Approach

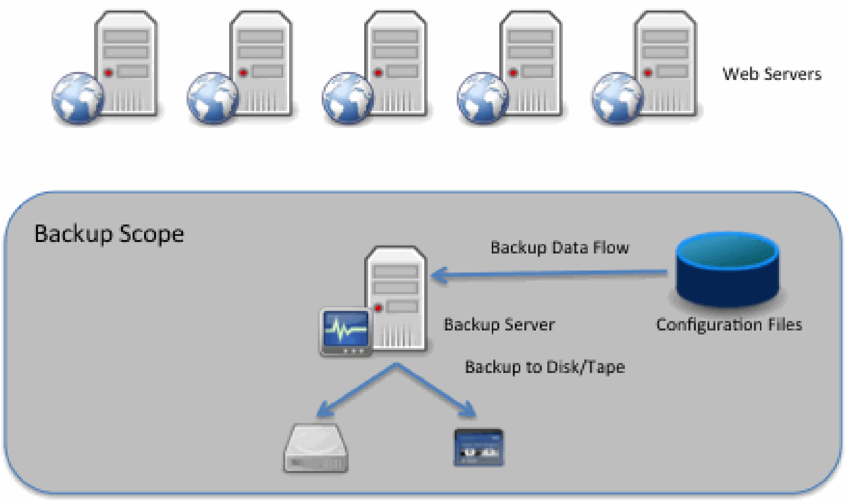


Figure – Amazon EC2 Backup Approach

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

Amazon Machine Image (AMI)

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

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

- Sharing the original AMI to another specified AWS account controlled by the customer.
- Starting a new instance based upon the shared AMI.

- Creating a new AMI from that running instance.

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

Configuration Files

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

Database and File Servers

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

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

Disaster Recovery

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

General Disaster Recovery/COOP and Backup Requirements and Issues

Some of the minimum needs and requirements in a traditional DR approach are:

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

AWS Capabilities for DR/COOP/Backup Solutions

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

AWS offers the following high-level DR capabilities:

- Fast Performance: Fast, disk-based storage and retrieval of files.
- No Tape: Eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software.
- Compliance: Minimize downtime to avoid breaching Service Level Agreements (SLAs).
- Elasticity: Add any amount of data, quickly. Easily expire and delete without handling media.
- Security: Secure and durable cloud DR platform with industry-recognized certifications and audits.
- Partners: AWS solution providers and system integration partners to help with deployments.

Solution Use Cases

AWS can enable customers to cost-effectively operate multiple DR strategies. Error! Reference source not found. shows a spectrum of scenarios—“backup & restore,” “pilot light,” “warm standby,” and “multi-site”—arranged by how quickly a system can be available to users after a DR event.

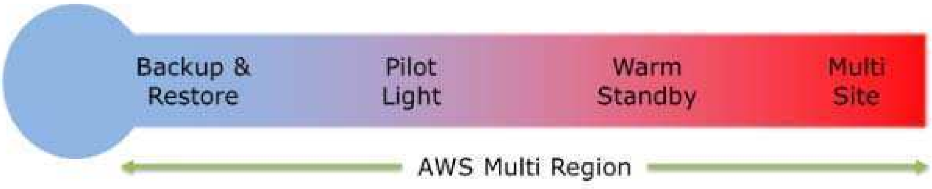


Figure – Spectrum of DR Options.

Each DR option is discussed in more detail below:

- Backup and Restore: In most traditional environments, data is backed up to tape and sent off-site regularly. Recovery time will be the longest using this method, and lack of automation leads to increased costs. Using Amazon Simple Storage Service (Amazon S3) is ideal for backup data, as it is designed to provide 99.999999999% durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. Also, with AWS Storage Gateway, customers can automatically back up on-premises data to Amazon S3.
- Pilot Light for Simple Recovery into AWS Warm Standby Solution: The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small idle flame that’s always on can quickly ignite the entire furnace to heat up a house as needed. This scenario is analogous to a backup and restore scenario; however, customers must ensure that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the

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

time comes for recovery, customers would rapidly provision a full-scale production environment around the critical core.

- Warm Standby Solution in AWS: The term "warm standby" is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. It further decreases recovery time because, in this case, some services are always running. By identifying business-critical systems, customers could fully duplicate these systems on AWS and have them always on.
- Multi-Site Solution Deployed on AWS and On-Site: A multi-site solution runs in AWS as well as on a customer's existing on-premise infrastructure in an active-active configuration. During a disaster situation, an organization can simply send all traffic to AWS servers, which can scale to handle their full production load.

DR Resources

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

- Read the AWS whitepaper Using AWS for Disaster Recovery
- Read the Forrester whitepaper File Storage Costs Less in the Cloud than In-House
- Review a sample AWS DR architecture

Review more information on AWS DR capabilities and approaches

CA Response:

For Agile and APIM - CA commits to the following data backup and replication during the Subscription Term:

Data Backup: All Customers of the Service offering shall have their data backed up on a daily basis. Backups are securely replicated to an alternate location (within the same geographic location) limiting data loss to no more than 24 hours in the event of a primary data location disaster.

- Daily backups are retained for 7 days
- Removable media are not used for data or backup storage
- Restoration of data may require engagement of CA Professional Services for an additional fee

In addition, snapshots of database transactions are taken every hour to a disaster recovery site allowing for emergency disaster recovery with maximum of 1.5 hours of data loss due to catastrophic onsite failure (fire in cage, natural disaster, etc. at data center). Backups are tested monthly and a full disaster recovery process to the offsite application cluster is tested semi-annually.

We manage systems through Chef and the configuration cookbooks are backed up. Backups are stored in our warm data center. We have a hot/warm data configuration with both data centers located within the US but ~1300 miles apart.

ASM - Backups are stored on disk only, sync'd between data centers for DR purposes. Automation tools are used to manage the configuration of ASM internal servers, and can be used for recovery. CA has an alternate site approximately 900 miles from our primary site. ASM has a warm standby with near time data replication between the data centers.

MAA – Backups are stored on disk only, sync'd between data centers for DR purposes. Automation tools are used to manage the configuration of MAA internal servers, and can be used for recovery. Daily differential and full backups reside in the primacy site with weekly data backups residing offsite. The MAA service is currently available from one data center only.

PPM - Nightly backups are stored on disk only. Server images are template based and are rebuilt as needed using automation. CA has an alternate site approximately 900 miles from our primary site. Nightly backups are encrypted and synchronized to the alternate data center via a secure tunnel. While CA PPM SaaS has global data centers, the location where data is stored and recovered to is within region as defined in the PPM SaaS Listing. For US based clients this region in within the US.

Microsoft Response:

Azure Backup is efficient over the network and on your disk. Once the initial seeding is complete, only incremental changes are sent at a defined frequency. Built-in features, such as compression, encryption, longer retention, and bandwidth throttling, help boost IT efficiency.

Azure Site Recovery protects server backups by automating the replication of the virtual machines based on policies that you set and control. Azure Site Recovery can protect Hyper-V, VMware and physical servers and you can use Azure or your secondary datacenter as your recovery site. Site Recovery coordinates and manages the ongoing replication of data by integrating with existing technologies including System Center and SQL Server AlwaysOn.

Azure has several datacenters in the United States and abroad. The customer has the ability to select where their data is stored and how many copies of that data are available.

8.9 DATA PROTECTION

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

SHI understands that data encryption requirements may vary and we will work with customers to classify data and decide if it needs to be encrypted and identify the best solutions.

8.9.1

Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

AWS Response:

AWS customers retain control and ownership of their data, and all data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers should consider the sensitivity of their data and decide if and how they will encrypt data while it is in transit and while it is at rest.

Securing Data at Rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions to manual, client-side options. Choosing the right solutions depends on which AWS cloud services are being used and customer requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide.

Additionally, the *Securing Data at Rest with Encryption* whitepaper provides an overview of the options for encrypting data at rest in AWS cloud services. It describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS cloud services.

Securing Data in Transit

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

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

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

CA Response:

Agile - All data in transit is encrypted. We support TLS 1+. For data at rest we have both database and disk level encryption. DB encryption utilizes Oracle TDE w/ AES-256.

APIM - All data is encrypted via TLS Mutual Authentication during transit

ASM - All data transmitted between data centers is encrypted in-transit. HTTPS/TLS is used by the ASM dashboard and API.

MAA - HTTPS/TLS encrypts the data in-transit. Sensitive data rest is encrypted using native encryption of SQL and NoSQL vendors.

PPM - All web traffic is protected by SHA256 bit TLS 1.0, 1.1, or 1.2 encryption and 2048 bit RSA public keys. The CA PPM SaaS application encrypts user session data. CA PPM SaaS email services supports TLS encryption.

Microsoft Response:

Azure offers security via Azure Active Directory, multifactor authentication, encryption and key management for data in transit and at rest, network security (vpn, acl), antimalware, centralized monitoring and penetration testing for all levels of users (Commercial, Government, Enterprise).

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.

SHI Response:

Upon award and request from a Purchasing Entity, we agree to review, discuss, and if applicable sign any necessary agreements associated with the purchase of products from this contract.

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.

AWS Response:

As part of the SHI/AWS solution, we will comply with terms in the Master Agreement which means we do not have access to any of the Purchasing Entity users' data.

CA Response:

CA Technologies hosts all customer data in secure multi-tenant or single tenant arrangements. All customer data is maintained in the strictest privacy according to CA Technologies policies, governance, SSAE 16 regulations. CA policies strictly prohibit the resale, redistribution or use by any third party of any and all customer data.

CA Technologies has written data security controls in place at CA Technologies to help ensure that Customer Data is appropriately protected and are applicable to SaaS operations.

Customer Data provided to CA Technologies is considered "Highly Confidential Information" under our Data Classification Policy and is afforded the highest level of security at the company.

CA Technologies has documented and implemented policies and procedures ("Policies and Procedures") that regulate the processing of Customer Data, including its receipt, transmission, storage, distribution, access and deletion. CA Technologies Policies and Procedures are designed to comply with all applicable laws, rules and regulations in the countries in which it conducts business.

CA Technologies maintains a comprehensive set of information security Policies and Procedures that are approved by senior management and are reviewed and updated to remain compliant with the law and current industry practices. These Policies and Procedures include:

- Organizational security

- Physical and environmental security
- Communications and connectivity
- Change control
- Data integrity
- Incident response
- Privacy
- Backup and offsite storage
- Vulnerability monitoring
- Information classification
- Data-handling; and
- Security configuration standards for networks, operating systems, applications and desktops

Microsoft Response:

Customer Data will be used only to provide customer the Online Services including purposes compatible with providing those services. For example, we may use Customer Data to provide a personalized experience, improve service reliability, combat spam or other malware, or improve features and functionality of the Online Services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, you or your end users through use of the Online Service. Customer Data is not Administrator Data, Payment Data, or Support Data.

8.10 SERVICE LEVEL AGREEMENTS

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response. Please not that each partner included with this response has specific SLAs associated with their solution and oftentimes are non-negotiable. SHI will work with customers to review and understand the SLAs of the solution that best fits their needs.

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 Response:

Our IaaS and PaaS service offer is continually updated and improved for compliance, performance, security, usability and generally better service. Purchasing Entities will hold on to negotiated SLAs that require lowered service than the IaaS and PaaS offers would provide over time.

AWS will give customers 6 months if at any time we decide to alter the SLA. It is important to note that in the past 10 years AWS has not deprecated the SLA but instead has improved it.

SHI agrees to proactively look at SLA and notify Purchasing Entities of any changes.

CA Response:

The target availability SLA of 99.8% is standard and not negotiable.

Microsoft Response:

The SLA's provided are nonnegotiable. Per Microsoft if the SLA is not met, they will offer a service credit based on the month of non-compliance.

8.10.2

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

AWS Response:

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

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

CA Response:

The target availability SLA of 99.8% is standard and not negotiable.

Microsoft Response:

Microsoft Azure Services

API Management Services

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given API Management instance has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all API Management instances deployed by you in a given Microsoft Azure subscription during a billing month.

"**Proxy**" is the component of the API Management Service responsible for receiving API requests and forwarding them to the configured dependent API.

Downtime: The total accumulated Deployment Minutes, across all API Management instances deployed by you in a given Microsoft Azure subscription, during which the API Management Service is unavailable. A minute is considered unavailable for a given API Management instance if all continuous attempts to perform operations through the Proxy throughout the minute result in either an Error Code or do not return a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit for Standard Tier:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit for Premium Tier deployments scaled across two or more regions:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

App Service

Additional Definitions:

"**App**" is a Web App deployed by Customer within the App Service, excluding web apps in the Free and Shared tiers.

"**Deployment Minutes**" is the total number of minutes that a given App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the App was created or the Customer initiated an action that would result in running the App to the time the Customer initiated an action that would result in stopping or deleting the Web App.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Apps deployed by Customer in a given Microsoft Azure subscription during a billing month

Downtime: is the total accumulated Deployment Minutes, across all Apps deployed by Customer in a given Microsoft Azure subscription, during which the App is unavailable. A minute is considered unavailable for a given App when there is no connectivity between the App and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Additional Terms: Service Credits are applicable only to fees attributable to your use of Apps and not to fees attributable to other types of apps available through the App Service, which are not covered by this SLA.

Application Gateway

Additional Definitions:

"**Application Gateway Cloud Service**" refers to a collection of one or more Application Gateway instances configured to perform HTTP load balancing services.

"**Maximum Available Minutes**" is the total accumulated minutes during a billing month during which an Application Gateway Cloud Service comprising two or more medium or larger Application Gateway instances has been deployed in a Microsoft Azure subscription.

Downtime: is the total accumulated Maximum Available Minutes during a billing month for a given Application Gateway Cloud Service during which the Application Gateway Cloud Service is unavailable. A given minute is considered unavailable if all attempts to connect to the Application Gateway Cloud Service throughout the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Automation Service

Additional Definitions:

"**Delayed Jobs**" is the total number of Jobs, for a given Microsoft Azure subscription, that fail to start within thirty (30) minutes of their Planned Start Times.

"**Job**" means the execution of a Runbook.

"**Planned Start Time**" is a time at which a Job is scheduled to begin executing.

"**Runbook**" means a set of actions specified by you to execute within Microsoft Azure.

"**Total Jobs**" is the total number of Jobs scheduled for execution during a given billing month, for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Jobs - Delayed\ Jobs}{Total\ Jobs}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Backup Service

Additional Definitions:

"**Backup**" or "**Back Up**" is the process of copying computer data from a registered server to a Backup Vault.

“**Backup Agent**” refers to the software installed on a registered server that enables the registered server to Back Up or Restore one or more Protected Items.

“**Backup Vault**” refers to a container in which you may register one or more Protected Items for Backup.

“**Deployment Minutes**” is the total number of minutes during which a Protected Item has been scheduled for Backup to a Backup Vault.

“**Failure**” means that either the Backup Agent or the Service fails to fully complete a properly configured Backup or Recovery operation due to unavailability of the Backup Service.

“**Maximum Available Minutes**” is the sum of all Deployment Minutes across all Protected Items for a given Microsoft Azure subscription during a billing month.

“**Protected Item**” refers to a collection of data, such as a volume, database, or virtual machine that has been scheduled for Backup to the Backup Service such that it is enumerated as a Protected Item in the Protected Items tab in the Recovery Services section of the Management Portal.

“**Recovery**” or “**Restore**” is the process of restoring computer data from a Backup Vault to a registered server.

Downtime: The total accumulated Deployment Minutes across all Protected Items scheduled for Backup by you in a given Microsoft Azure subscription during which the Backup Service is unavailable for the Protected Item. The Backup Service is considered unavailable for a given Protected Item from the first Failure to Back Up or Restore the Protected Item until the initiation of a successful Backup or Recovery of a Protected Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Batch Service

Additional Definitions:

“Average Error Rate” for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

“**Excluded Requests**” are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"**Failed Requests**" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

“**Total Requests**” is the total number of authenticated REST API requests, other than Excluded Requests, to perform operations against Batch accounts attempted within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\textit{100\% - Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

BizTalk Services

Additional Definitions:

"**BizTalk Service Environment**" refers to a deployment of the BizTalk Services created by you, as represented in the Management Portal, to which you may send runtime message requests.

"**Deployment Minutes**" is the total number of minutes that a given BizTalk Service Environment has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription during a billing month.

"**Monitoring Storage Account**" refers to the Azure Storage account used by the BizTalk Services to store monitoring information related to the execution of the BizTalk Services.

Downtime: The total accumulated Deployment Minutes, across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription, during which the BizTalk Service Environment is unavailable. A minute is considered unavailable for a given BizTalk Service Environment when there is no connectivity between your BizTalk Service Environment and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x \; 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic, Standard, and Premium tiers of the BizTalk Services. The Developer tier of the Microsoft Azure BizTalk Services is not covered by this SLA.

Additional Terms: When submitting a claim, you must ensure that complete monitoring data is maintained within the Monitoring Storage Account and is made available to Microsoft.

Cache Services

Additional Definitions:

"**Cache**" refers to a deployment of the Cache Service created by you, such that its Cache Endpoints are enumerated in the Cache tab in the Management Portal.

"**Cache Endpoints**" refers to endpoints through which a Cache may be accessed.

"**Deployment Minutes**" is the total number of minutes that a given Cache has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Caches deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Caches deployed by you in a given Microsoft Azure subscription, during which the Cache is unavailable. A minute is considered unavailable for a given Cache when there is no connectivity throughout the minute between one or more Cache Endpoints associated with the Cache and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x \; 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%

Monthly Uptime Percentage	Service Credit
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Cache Service, which includes the Azure Managed Cache Service or the Standard tier of the Azure Redis Cache Service. The Basic tier of the Azure Redis Cache Service is not covered by this SLA.

CDN Service

Downtime To assess Downtime, Microsoft will review data from any commercially reasonable independent measurement system used by you.

You must select a set of agents from the measurement system's list of standard agents that are generally available and represent at least five geographically diverse locations in major worldwide metropolitan areas (excluding PR of China).

Measurement System tests (frequency of at least one test per hour per agent) will be configured to perform one HTTP GET operation according to the model below:

1. A test file will be placed on your origin (e.g., Azure Storage account).
2. The GET operation will retrieve the file through the CDN Service, by requesting the object from the appropriate Microsoft Azure domain name hostname.
3. The test file will meet the following criteria:

i. The test object will allow caching by including explicit "Cache-control: public" headers, or lack of "Cache-Control: private" header.

ii. The test object will be a file at least 50KB in size and no larger than 1MB.

iii. Raw data will be trimmed to eliminate any measurements that came from an agent experiencing technical problems during the measurement period.

Monthly Uptime Percentage: The percentage of HTTP transactions in which the CDN responds to client requests and delivers the requested content without error. Monthly Uptime Percentage of the CDN Service is calculated as the number of times the object was delivered successfully divided by the total number of requests (after removing erroneous data).

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99.5%	25%

Cloud Services

Additional Definitions:

"Cloud Services" refers to a set of compute resources utilized for Web and Worker Roles.

"Maximum Available Minutes" is the total accumulated minutes during a billing month for all Internet facing roles that have two or more instances deployed in different Update Domains. Maximum Available Minutes is measured from when the Tenant has been deployed and its associated roles have been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Tenant.

"Tenant" represents one or more roles each consisting of one or more role instances that are deployed in a single package.

"Update Domain" refers to a set of Microsoft Azure instances to which platform updates are concurrently applied.

"Web Role" is a Cloud Services component run in the Azure execution environment that is customized for web application programming as supported by IIS and ASP.NET.

"Worker Role" is a Cloud Services component run in the Azure execution environment that is useful for generalized development, and may perform background processing for a Web Role.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\mathit{Maximum\ Available\ Minutes\text{-}Downtime}}{\mathit{Maximum\ Available\ Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Data Factory – Activity Runs

Additional Definitions:

Activity Run means the execution or attempted execution of an activity

Delayed Activity Runs is the total number of attempted Activity Runs in which an activity fails to begin executing within four (4) minutes after the time at which it is scheduled for execution and all dependencies that are prerequisite to execution have been satisfied.

Total Activity Runs is the total number of Activity Runs attempted during in a billing month for a given Microsoft Azure Subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Activity\ Runs - Delayed\ Activty\ Runs}{Total\ Activity\ Runs}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Data Factory – API Calls

Additional Definitions:

Excluded Requests is the set of requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

Failed Requests is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or otherwise fail to return a Success Code within two minutes.

Resources means pipelines, data sets, and linked services created within a Data Factory.

Total Requests is the set of all requests, other than Excluded Requests, to perform operations against Resources within active pipelines during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Requests - Failed\ Requests}{Total\ Requests}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

DocumentDB

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Database Account**" is a DocumentDB account containing one or more databases.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests, across all Resources in a given Azure subscription, during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"**Failed Requests**" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

"**Resource**" is a set of URI addressable entities associated with a Database Account. .

"**Total Request**" is the set of all requests, other than Excluded Requests, to perform operations issued against Resources attempted within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% \text{ - } Average\ Error\ Rate$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

ExpressRoute

Additional Definitions:

"**Dedicated Circuit**" means a logical representation of connectivity offered through the ExpressRoute Service between your premises and Microsoft Azure through an exchange provider or a network service provider, where such connectivity does not traverse the public Internet.

"**Maximum Available Minutes**" is the total number of minutes that a given Dedicated Circuit is linked to one or more Virtual Networks in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

"**Virtual Network**" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

"**VPN Gateway**" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: The total accumulated minutes during a billing month for a given Microsoft Azure subscription during which the Dedicated Circuit is unavailable. A minute is considered unavailable for a given Dedicated Circuit if all attempts by you within the minute to establish IP-level connectivity to the VPN Gateway associated with the Virtual Network fail for longer than thirty seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes} \ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Uptime Percentage and Service Credits are calculated for each Dedicated Circuit used by you.

HDInsight

Additional Definitions:

"**Cluster Internet Gateway**" means a set of virtual machines within an HDInsight Cluster that proxy all connectivity requests to the Cluster.

"**Deployment Minutes**" is the total number of minutes that a given HDInsight Cluster has been deployed in Microsoft Azure.

"**HDInsight Cluster**" or "**Cluster**" means a collection of virtual machines running a single instance of the HDInsight Service.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Clusters deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes when the HDInsight Service is unavailable. A minute is considered unavailable for a given Cluster if all continual attempts within the minute to establish a connection to the Cluster Internet Gateway fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Key Vault

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given key vault has been deployed in Microsoft Azure during a billing month.

"**Excluded Transactions**" are transactions for creating, updating, or deleting key vaults, keys, or secrets.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Key Vaults deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated Deployment Minutes, across all key vaults deployed by Customer in a given Microsoft Azure subscription, during which the key vault is unavailable. A minute is considered unavailable for a given key vault if all continuous attempts to perform transactions, other than Excluded Transactions, on the key vault throughout the minute either return an Error Code or do not result in a Success Code within 5 seconds from Microsoft's receipt of the request.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Machine Learning – Batch Execution Service (BES) and Management APIs Service

Additional Definitions:

"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code.

"**Total Transaction Attempts**" is the total number of authenticated REST BES and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning BES and Management API Service. The Free Machine Learning tier is not covered by this SLA.

Machine Learning – Request Response Service (RRS)

Additional Definitions:

"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code.

"**Total Transaction Attempts**" is the total number of authenticated REST RRS and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning RRS and Management API Service. The Free Machine Learning tier is not covered by this SLA.

Media Services – Content Protection Service

Additional Definitions:

"**Failed Transactions**" are all Valid Key Requests included in Total Transaction Attempts that result in an Error Code or otherwise do not return a Success Code within 30 seconds after receipt by the Content Protection Service.

"**Total Transaction Attempts**" are all Valid Key Requests made by you during a billing month for a given Azure subscription.

"Valid Key Requests" are all requests made to the Content Protection Service for existing content keys in a Customer's Media Service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Media Services – Encoding Service

Additional Definitions:

"**Encoding**" means the processing of media files per subscription as configured in the Media Services Tasks.

"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that do not return a Success Code within 30 seconds from Microsoft's receipt of the request.

"**Media Service**" means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

"**Media Services Task**" means an individual operation of media processing work as configured by you. Media processing operations involve encoding and converting media files.

"**Total Transaction Attempts**" is the total number of authenticated REST API requests with respect to a Media Service made by you during a billing month for a subscription. Total Transaction Attempts does not include REST API requests that return an Error Code that are continuously repeated within a five-minute window after the first Error Code is received.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Media Services – Indexer Service

Additional Definitions:

"**Encoding Reserved Unit**" means encoding reserved units purchased by the customer in an Azure Media Services account

"**Failed Transactions**" is the set of Indexer Tasks within Total Transaction Attempts that either, a) do not complete within a time period that is 3 times the duration of the input file, or b) do not start processing within 5 minutes of the time that an Encoding Reserved Unit becomes available for use by the Indexer Task.

"**Indexer Task**" means a Media Services Task that is configured to index an MP3 input file with a minimum five-minute duration.

"**Total Transaction Attempts**" is the total number of Indexer Tasks attempted to be executed using an available Encoding Reserved Unit by Customer during a billing month for a subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Media Services – Live Channels

Additional Definitions:

"**Channel**" means an end point within a Media Service that is configured to receive media data.

"**Deployment Minutes**" is the total number of minutes that a given Channel has been purchased and allocated to a Media Service and is in a running state during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Channels purchased and allocated to a Media Service during a billing month.

"**Media Service**" means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

Downtime: The total accumulated Deployment Minutes when the Live Channels Service is unavailable. A minute is considered unavailable for a given Channel if the Channel has no External Connectivity during the minute.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Media Services – Streaming Service

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Streaming Unit has been purchased and allocated to a Media Service during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Streaming Units purchased and allocated to a Media Service during a billing month.

"**Media Service**" means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

"**Media Service Request**" means a request issued to your Media Service.

"**Streaming Unit**" means a unit of reserved egress capacity purchased by you for a Media Service.

"**Valid Media Services Requests**" are all qualifying Media Service Requests for existing media content in a customer's Azure Storage account associated with its Media Service when at least one Streaming Unit has been purchased and allocated to that Media Service. Valid Media Services Requests do not include Media Service Requests for which total throughput exceeds 80% of the Allocated Bandwidth.

Downtime: The total accumulated Deployment Minutes when the Streaming Service is unavailable. A minute is considered unavailable for a given Streaming Unit if all continuous Valid Media Service Requests made to the Streaming Unit throughout the minute result in an Error Code.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Mobile Engagement

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" is the set of REST API requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"**Failed Requests**" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 30 seconds.

"**Mobile Engagement Application**" is an Azure Mobile Engagement service instance.

"**Total Requests**" is the total number of authenticated REST API requests, other than Excluded Requests, made to Mobile Engagement Applications within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

The Free Mobile Engagement tier is not covered by this SLA.

Mobile Services

Additional Definitions:

"**Failed Transactions**" include any API calls included in Total Transaction Attempts that result in either an Error Code or do not return a Success Code.

"**Total Transaction Attempts**" are the total accumulated API calls made to the Azure Mobile Services during a billing month for a given Microsoft Azure subscription for which the Azure Mobile Services are running.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Standard and Premium Mobile Services tiers. The Free Mobile Services tier is not covered by this SLA.

Multi-Factor Authentication Service

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Multi-Factor Authentication provider has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription, during which the Multi-Factor Authentication Service is unable to receive or process authentication requests for the Multi-Factor Authentication provider.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%

Monthly Uptime Percentage	Service Credit
< 99%	25%

Operational Insights

Additional Definitions:

"Batch" means a group of Log Data entries that are either uploaded to the Operational Insights Service or read from storage by the Operational Insights Service within a given period of time. Batches queued for indexing are displayed in the usage section of the Management Portal.

"Log Data" refers to information regarding a supported event, such as IIS and Windows events, that is logged by a computer and for which the Operational Insights Service has been configured to be processed by the Service index.

"Delayed Batches" is the total number of Batches within Total Queued Batches that fail to complete indexing within six hours of the Batch being queued.

"Total Queued Batches" is the total number of Batches queued for indexing by the Operational Insights Service during a given billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Queued\ Batches - Delayed\ Batches}{Total\ Queued\ Batches}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

RemoteApp

Additional Definitions:

"**Application**" means a software application that is configured for streaming to a device using the RemoteApp Service.

"**Maximum Available Minutes**" is the sum of all User Application Minutes across all Users granted access to one or more Applications in a given Azure subscription during a billing month.

"**User**" means a specific user account that is able to stream an Application using the RemoteApp Service, as enumerated in the Management Portal.

"**User Application Minutes**" is the total number of minutes in a billing month during which you have granted a User access to an Application.

Downtime: The total accumulated User Minutes during which the RemoteApp Service is unavailable. A minute is considered unavailable for a given User when the User is unable to establish connectivity to an Application.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the RemoteApp Service. The RemoteApp free trial is not covered by this SLA.

Scheduler

Additional Definitions:

"**Maximum Available Minutes**" is the total number of minutes in a billing month.

"**Planned Execution Time**" is a time at which a Scheduled Job is scheduled to begin executing.

"**Scheduled Job**" means an action specified by you to execute within Microsoft Azure according to a specified schedule.

Downtime: The total accumulated minutes in a billing month during which one or more of your Scheduled Jobs is in a state of delayed execution. A given Scheduled Job is in a state of delayed execution if it has not begun executing after a Planned Execution Time, provided that such delayed execution time shall not be considered Downtime if the Scheduled Job begins executing within thirty (30) minutes after a Planned Execution Time.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Search

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests, across all Search Service Instances in a given Azure subscription, during a given one-hour interval. If the Total Requests in a one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" are all requests that are throttled due to exhaustion of resources allocated for a Search Service Instance, as indicated by an HTTP 503 status code and a response header indicating the request was throttled.

"**Failed Requests**" is the set of all requests within Total Requests that fail to return either a Success Code or HTTP 4xx response.

"**Replica**" is a copy of a search index within a Search Service Instance.

"**Search Service Instance**" is an Azure Search service instance containing one or more search indexes.

"**Total Requests**" is the set of (i) all requests to update a Search Service Instance having three or more Replicas, plus (ii) all requests to query a Search Service Instance having two or more Replicas, other than Excluded Requests, within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Free Search tier is not covered by this SLA.

Service-Bus Service – Event Hubs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Event Hub has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers during a billing month.

"**Message**" refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers, during which the Event Hub is unavailable. A minute is considered unavailable for a given Event Hub if all continuous attempts to send or receive Messages or perform other operations on the Event Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\mathit{Maximum\ Available\ Minutes\text{-}Downtime}}{\mathit{Maximum\ Available\ Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Event Hubs tiers. The Free Event Hubs tier is not covered by this SLA.

Service-Bus Service – Notification Hubs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Notification Hub has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers, during which the Notification Hub is unavailable. A minute is considered unavailable for a given Notification Hub if all continuous attempts to send notifications or perform registration management operations with respect to the Notification Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\mathit{Maximum\ Available\ Minutes\text{-}Downtime}}{\mathit{Maximum\ Available\ Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Notification Hubs tiers. The Free Notification Hubs tier is not covered by this SLA.

Service-Bus Service – Queues and Topics

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Queue or Topic has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Queues and Topics deployed by you in a given Microsoft Azure subscription during a billing month.

"**Message**" refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Queues and Topics deployed by you in a given Microsoft Azure subscription, during which the Queue or Topic is unavailable. A minute is considered unavailable for a given Queue or Topic if all continuous attempts to send or receive Messages or perform other operations on the Queue or Topic throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service-Bus Service – Relays

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Relay has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Relays deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Relays deployed by you in a given Microsoft Azure subscription, during which the Relay is unavailable. A minute is considered unavailable for a given Relay if all continuous attempts to establish a connection to the Relay throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Site Recovery Service – On-Premises-to-Azure

Additional Definitions:

"**Failover**" is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

"**On-Premises-to-Azure Failover**" is the Failover of a Protected Instance from a non-Azure primary site to an Azure secondary site. You may designate a particular Azure datacenter as a secondary site, provided that if Failover to the designated datacenter is not possible, Microsoft may replicate to a different datacenter in the same region.

"**Protected Instance**" refers to a virtual or physical machine configured for replication by the Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

"**Recovery Time Objective (RTO)**" means the period of time beginning when you initiate a Failover of a Protected Instance experiencing either a planned or unplanned outage for On-Premises-to-Azure replication to the time when the Protected Instance is running as a virtual machine in Microsoft Azure, excluding any time associated with manual action or the execution of your scripts.

Monthly Recovery Time Objective: The Monthly Recovery Time Objective for a specific Protected Instance configured for On-Premises-to-Azure replication in a given billing month is four hours for an unencrypted Protected Instance and six hours for an encrypted Protected Instance. One hour will be added to the monthly Recovery Time Objective for each additional 25GB over the initial 100GB Protected Instance size.

Service Credit (Assuming Protected Instance of 100GB, or less):

Protected Instance	Monthly Recovery Time Objective	Service Credit
Unencrypted	> 4 hours	100%
Encrypted	> 6 hours	100%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

Site Recovery Service – On-Premises-to-On-Premises

Additional Definitions:

"**Failover**" is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

"**Failover Minutes**" is the total number of minutes in a billing month during which a Failover of a Protected Instance configured for On-Premises-to-On-Premises replication has been attempted but not completed.

"**Maximum Available Minutes**" is the total number of minutes that a given Protected Instance has been configured for On-Premises-to-On-Premises replication by the Site Recovery Service during a billing month.

"**On-Premises-to-On-Premises Failover**" is the Failover of a Protected Instance from a non-Azure primary site to a non-Azure secondary site.

"**Protected Instance**" refers to a virtual or physical machine configured for replication by the Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

Downtime: The total accumulated Failover Minutes in which the Failover of a Protected Instance is unsuccessful due to unavailability of the Site Recovery Service, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

SQL Database Service (Basic, Standard and Premium Tiers)

Additional Definitions:

"**Database**" means any Basic, Standard, or Premium Microsoft Azure SQL Database.

"**Deployment Minutes**" is the total number of minutes that a given Basic, Standard, or Premium Database has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Basic, Standard, and Premium Databases for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes across all Basic, Standard, and Premium Databases deployed by you in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by you to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\; x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

SQL Database Service (Web and Business Tiers)

Additional Definitions:

"**Database**" means any Web or Business Microsoft Azure SQL Database.

"**Deployment Minutes**" is the total number of minutes that a given Web or Business Database has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Web and Business Databases for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes across all Web and Business Databases deployed by you in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by you to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\; x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Storage Service

Additional Definitions:

"**Average Error Rate"** for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Excluded Transactions**" are storage transactions that do not count toward either Total Storage Transactions or Failed Storage Transactions. Excluded Transactions include pre-authentication failures; authentication failures; attempted transactions for storage accounts over their prescribed quotas; creation or deletion of containers, tables, or queues; clearing of queues; and copying blobs between storage accounts.

"**Error Rate**" is the total number of Failed Storage Transactions divided by the Total Storage Transactions during a set time interval (currently set at one hour). If the Total Storage Transactions in a given one-hour interval is zero, the error rate for that interval is 0%.

"**Failed Storage Transactions**" is the set of all storage transactions within Total Storage Transactions that are not completed within the Maximum Processing Time associated with their respective transaction type, as specified in the table below. Maximum Processing Time includes only the time spent processing a transaction request within the Storage Service and does not include any time spent transferring the request to or from the Storage Service.

Request Types	Maximum Processing Time
PutBlob and GetBlob (includes blocks and pages) Get Valid Page Blob Ranges	Two (2) seconds multiplied by the number of MBs transferred in the course of processing the request
Copy Blob	Ninety (90) seconds (where the source and destination blobs are within the same storage account)
PutBlockList GetBlockList	Sixty (60) seconds
Table Query List Operations	Ten (10) seconds (to complete processing or return a continuation)
Batch Table Operations	Thirty (30) seconds
All Single Entity Table Operations All other Blob and Message Operations	Two (2) seconds

These figures represent maximum processing times. Actual and average times are expected to be much lower.

Failed Storage Transactions do not include:

1. Transaction requests that are throttled by the Storage Service due to a failure to obey appropriate back-off principles.
2. Transaction requests having timeouts set lower than the respective Maximum Processing Times specified above.
3. Read transactions requests to RA-GRS Accounts for which you did not attempt to execute the request against Secondary Region associated with the storage account if the request to the Primary Region was not successful.
4. Read transaction requests to RA-GRS Accounts that fail due to Geo-Replication Lag.

"**Geo Replication Lag**" for GRS and RA-GRS Accounts is the time it takes for data stored in the Primary Region of the storage account to replicate to the Secondary Region of the storage account. Because GRS and RA-GRS Accounts are replicated asynchronously to the Secondary Region, data written to the Primary Region of the storage account will not be immediately available in the Secondary Region. You can query the Geo Replication Lag for a storage account, but Microsoft does not provide any guarantees as to the length of any Geo Replication Lag under this SLA.

"**Geographically Redundant Storage (GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You cannot directly read data from or write data to the Secondary Region associated with GRS Accounts.

"**Locally Redundant Storage (LRS) Account**" is a storage account for which data is replicated synchronously only within a Primary Region.

"**Primary Region**" is a geographical region in which data within a storage account is located, as selected by you when creating the storage account. You may execute write requests only against data stored within the Primary Region associated with storage accounts.

"**Read Access Geographically Redundant Storage (RA-GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You can directly read data from, but cannot write data to, the Secondary Region associated with RA-GRS Accounts.

"**Secondary Region**" is a geographical region in which data within a GRS or RA-GRS Account is replicated and stored, as assigned by Microsoft Azure based on the Primary Region associated with the storage account. You cannot specify the Secondary Region associated with storage accounts.

"**Total Storage Transactions**" is the set of all storage transactions, other than Excluded Transactions, attempted within a one-hour interval across all storage accounts in the Storage Service in a given subscription.

"**Zone Redundant Storage (ZRS) Account**" is a storage account for which data is replicated across multiple facilities. These facilities may be within the same geographical region or across two geographical regions.

Monthly Uptime Percentage: Monthly Uptime Percentage is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit – LRS, ZRS, GRS and RA-GRS (write requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit – RA-GRS (read requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

StorSimple Service

Additional Definitions:

"**Backup**" is the process of backing up data stored on a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

"**Cloud Tiering**" is the process of transferring data from a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

"**Deployment Minutes**" is the total number of minutes during which a Managed Item has been configured for Backup or Cloud Tiering to a StorSimple storage account in Microsoft Azure.

"**Failure**" means the inability to fully complete a properly configured Backup, Tiering, or Restoring operation due to unavailability of the StorSimple Service.

"**Managed Item**" refers to a volume that has been configured to Backup to the cloud storage accounts using the StorSimple Service.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Managed Items for a given Microsoft Azure subscription during a billing month.

"**Restoring**" is the process of copying data to a registered StorSimple device from its associated cloud storage account(s).

Downtime: The total accumulated Deployment Minutes across all Managed Items configured for Backup or Cloud Tiering by you in a given Microsoft Azure subscription during which the StorSimple Service is unavailable for the Managed Item. The StorSimple Service is considered unavailable for a given Managed Item from the first Failure of a Backup, Cloud Tiering, or Restoring operation with respect to the Managed Item until the initiation of a successful Backup, Cloud Tiering, or Restoring operation of the Managed Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Stream Analytics – API Calls

Additional Definitions:

"**Total Transaction Attempts**" is the total number of authenticated REST API requests to manage a streaming job within the Stream Analytics Service by Customer during a billing month for a given Microsoft Azure subscription.

"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code or otherwise do not return a Success Code within five minutes from Microsoft's receipt of the request.

"**Monthly Uptime Percentage**" for API calls within the Stream Analytics Service is represented by the following formula:

$$\text{Monthly Uptime \%} = \frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Stream Analytics – Jobs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given job has been deployed within the Stream Analytics Service during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all jobs deployed by Customer in a given Microsoft Azure subscription during a billing month.

Downtime is the total accumulated Deployment Minutes, across all jobs deployed by Customer in a given Microsoft Azure subscription, during which the job is unavailable. A minute is considered unavailable for a deployed job if the job is neither processing data nor available to process data throughout the minute.

"**Monthly Uptime Percentage**" for jobs within the Stream Analytics Service is represented by the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Traffic Manager Service

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Traffic Manager Profile has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Traffic Manager Profiles deployed by you in a given Microsoft Azure subscription during a billing month.

"**Traffic Manager Profile**" or "**Profile**" refers to a deployment of the Traffic Manager Service created by you containing a domain name, endpoints, and other configuration settings, as represented in the Management Portal.

"**Valid DNS Response**" means a DNS response, received from at least one of the Traffic Manager Service name server clusters, to a DNS request for the domain name specified for a given Traffic Manager Profile.

Downtime: The total accumulated Deployment Minutes, across all Profiles deployed by you in a given Microsoft Azure subscription, during which the Profile is unavailable. A minute is considered unavailable for a given Profile if all continual DNS queries for the DNS name specified in the Profile that are made throughout the minute do not result in a Valid DNS Response within two seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Virtual Machines

Additional Definitions:

"**Availability Set**" refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.

"**Fault Domain**" is a collection of servers that share common resources such as power and network connectivity.

"**Maximum Available Minutes**" is the total accumulated minutes during a billing month for all Internet facing Virtual Machines that have two or more instances deployed in the same Availability Set. Maximum Available Minutes is measured from when at least two Virtual Machines in the same Availability Set have both been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Virtual Machines.

"**Virtual Machine**" refers to persistent instance types that can be deployed individually or as part of an Availability Set.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

VPN Gateway

Additional Definitions:

"**Maximum Available Minutes**" is the total accumulated minutes during a billing month which a given VPN Gateway has been deployed in a Microsoft Azure subscription.

"**Virtual Network**" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

"**VPN Gateway**" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: Is the total accumulated VPN Gateway Maximum Available Minutes during which a VPN Gateway is unavailable. A minute is considered unavailable if all attempts to connect to the VPN Gateway within a thirty-second window within the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Visual Studio Online – Build Service

Additional Definitions:

"**Build Service**" is a feature that allows customers to build their applications in Visual Studio Online.

"**Maximum Available Minutes**" is the total number of minutes for which the paid Build Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Build Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Build Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Visual Studio Online – Load Testing Service

Additional Definitions:

"**Load Testing Service**" is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

"**Maximum Available Minutes**" is the total number of minutes for which the paid Load Testing Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Load Testing Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Load Testing Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Visual Studio Online – User Plans Service

Additional Definitions:

"**Build Service**" is a feature that allows customers to build their applications in Visual Studio Online.

"**Deployment Minutes**" is the total number of minutes for which a User Plan has been purchased during a billing month.

"**Load Testing Service**" is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all User Plans for a given Microsoft Azure subscription during a billing month.

"**User Plan**" refers to the set of features and capabilities selected for a user within a Visual Studio Online account in a Customer subscription. User Plan options and the features and capabilities per User Plan are described on the http://www.visualstudio.com website.

Downtime: The total accumulated Deployment Minutes, across all User Plans for a given Microsoft Azure subscription, during which the User Plan is unavailable. A minute is considered unavailable for a given User Plan if all continuous HTTP requests to perform operations, other than operations pertaining to the Build Service or the Load Testing Service, throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

8.11 DATA DISPOSAL

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

SHI Response:

SHI has data disposal services available to help customers meet compliance requirements and ensure safety of private data. SHI agrees to work with Purchasing Entities to review all available options related to their request.

AWS Response:

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

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

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

AWS Storage Device Decommissioning

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

CA Response:

Agile - A component of our strategy includes disk encryption for data at rest. This provides an additional safeguard that data is protected in the retirement stage of hardware, but our primary control is to utilize a 3rd party service that certifies destruction according to industry standards.

APIM – All Data is held with AWS. Data disposal is outlined in AWS's annual SOC 3 audits. A copy of the latest SOC 3 report can be found here:
http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

ASM, MAA, and PPM – All electronic media containing CA Technologies or customer sensitive data must be disposed of using approved techniques for proper sanitization. Data storage media is sanitized when hardware breaks, customers ask for sanitization to be performed, or when data storage media leaves data center's premises. Note, customer data is only stored on disk, so there is no process necessary for other media (e.g. USB, CD, and DVD). Secure media sanitization is processed through a vendor provided data destruction program.

All CA Technologies staff must ensure that any sensitive data stored on hard disks or other electronic media are properly disposed of using one of the approved techniques:

- Overwriting the media using DOD accepted software
- Degauss of the media
- Physically destroying the media rendering it unusable

Microsoft Response:

Microsoft follows strict standards and specific processes for removing customer data from all systems under our control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware.

Customers can retrieve a copy of all customer data at any time and for any reason without any assistance or notification required from Microsoft.

Microsoft contractually commits to specific processes when a customer leaves the service or the subscription expires. This includes deleting customer data from all systems under our control.

- If you, the customer, terminate your subscription or it expires (except for free trials), Microsoft will store your customer data in a limited-function account for 90 days (the retention period) to give you time to export the data or renew your subscription. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data.
- After this 90-day retention period, Microsoft will disable the account and delete all customer data, including any cached or backup copies. For in-scope services and Azure services, that deletion will occur within 90 days of the end of the retention period. (In-scope services are defined in the Data Processing Terms section of our Online Services Terms.)

In the multitenant environments of Microsoft enterprise cloud services, we take careful measures to logically separate customer data to help prevent one customer's data from leaking into the data of another customer, as well as to help block any customer from accessing another customer's deleted data.

When a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. All of the data on the drive is completely overwritten to ensure that the data cannot be recovered by any means.

When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

8.12 PERFORMANCE MEASURES AND REPORTING

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

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 Response:

SHI's performance and reporting capabilities draw on the repository of metadata retained by AWS' IaaS and PaaS service platform. Although there is currently no direct SLA published for performance and reporting metadata, the metadata is stored in AWS' S3 storage subcategory service which offers eleven-nines of durability.   Any missing performance and reporting can be easily reproduced to deliver the desired 99.9% or greater availability.

CA Response:

Agile - For Rally SaaS Unlimited Edition customers, our goal is to provide 99.9% up-time during each calendar quarter. If in any calendar quarter an up-time of 99.5% is not met and our customers were negatively impacted (for example, were unable to login to Rally), we will provide a service credit equal to one month of fees for use of the Rally Service.

APIM, ASM, MAA, and PPM – CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.

Microsoft Response:

Please see the response to 8.10.2 for details.

8.12.2

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

AWS Response:

Our support and service detailed above apply to Performance and Reporting:

- Quality assurance measures:
  - Average contacts to resolution
  - Average response time

Escalation plan:

- Dedicated resource escalates to SE immediately upon receipt of case, if requested by user, or if SLA is missed.
- Support Engineer (SE) resource escalates to Sr. Support Engineer immediately upon receipt of case, if requested by user, or if second SLA is missed.
- Sr. Support Engineer escalates to AWS engineering if SLA is missed.
- Dedicated resource and highest Engineer resources is engaged on the case until completed and closed by the user.

SLA = <12 hour response time

CA Response:

Agile – See response for 8.12.1

APIM, ASM, MAA, and PPM – Uptime SLA target is 99.8%

CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.

Microsoft Response:

Please see the response to 8.4.1 for details.

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.

AWS Response:

Our contact mediums for Performance and Reporting are:

- Email to support hunt-group
- Phone to designated contact representative

Escalation plan:

- Dedicated resource escalates to SE immediately upon receipt of case, if requested by user, or if SLA is missed.
- Support Engineer (SE) resource escalates to Sr. Support Engineer immediately upon receipt of case, if requested by user, or if second SLA is missed.
- Sr. Support Engineer escalates to AWS engineering if SLA is missed.

- Dedicated resource and highest Engineer resources is engaged on the case until completed and closed by the user.

SLA = <12 hour response time

CA Response:

CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc.

While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported.

Microsoft Response:

Support is provided by Microsoft at an additional cost. Please see the responses to 8.4.1 and 8.4.2 for details.

8.12.4

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

AWS Response:

SHI will automatically escalate missed SLA windows, and will work with Purchasing Entity users to accommodate desired resolution for Performance and Reporting functionality.

CA Response:

In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the contract.

Microsoft Response:

SLA remedies are covered in our response to question 8.10.2. Response times are covered in our response to question 8.4.2

8.12.5

Intentionally Deleted.

8.12.6

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

AWS Response:

Due to the nature of IaaS and PaaS, SHI and AWS seldom require client action for any updates or maintenance to Performance and Reporting functionality. However, we notify of any planned downtime via email within reasonably adequate timeframes, and respond to client users on a case by case basis to minimize any impact.

CA Response:

Agile - Regularly scheduled maintenance (planned downtime for upgrades and maintenance) where the customer has been given at least eight (8) hours notice does not count as downtime. Unscheduled maintenance, in which the Rally Service is unavailable and advance notice was not provided to customers, will be counted against the up-time SLA.

APIM - Planned downtime is scheduled and customers are notified in advance.

ASM - Customers are notified at least two weeks in advance for planned downtime.

MAA - Customers are notified at least two weeks in advance for planned downtime.

PPM - Maintenance falls into three categories:

- Monthly: Monthly maintenance windows are scheduled at least 3 months in advance and occur one Saturday each month. Maintenance windows are scheduled during local non-business hours. There is limited client input over these scheduled windows as infrastructure maintenance performed during these windows may impact multiple or all clients. Security patches and other operating system updates are applied during these windows. A reminder notification will be sent 7-10 days prior to these maintenance windows.
- Critical Scheduled: Periodically, a critical scheduled maintenance involving security or system stability may be required. A 72 hour notice will be provided to customers for these activities. In many cases this maintenance activities can be more flexibly timed to meet customer business needs. CA will provide reasonable accommodations to these types of maintenance periods where possible.
- Unplanned: Unplanned downtime is any loss of production system availability that does not have at least 72 hours advance notice to clients. These downtimes are generally system fault type issues but can also be proactive, emergency maintenance performed to prevent a system failure from occurring. Notices of service interruption will be sent as soon as the maintenance is scheduled or monitoring has determined a client's system is unavailable; a minimum of 24 hour notice is provided when practical. These types of downtime count against the client's uptime SLA and, therefore, are infrequent.

Microsoft Response:

The procedure would be discussed during the support call as outlined in 8.4.2

8.12.7

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

AWS Response:

SHI will automatically escalate missed SLA windows, and will work with Purchasing Entity users to accommodate desired resolution for Performance and Reporting functionality.

CA Response:

Defined monetary penalties are provided in the SaaS Listing document.

Microsoft Response:

The financial consequences are detailed in our response 8.10.2.

8.12.8

Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

AWS Response:

Performance reports are available via the Web, and report metrics are available in 5-minute intervals.

CA Response:

Agile - Real-time and historical system status can be viewed at https://status.rallydev.com

APIM – A report of the Service's measured monthly SLA is available to Customer upon request

ASM – Reports can be generated periodically and ad hoc.

MAA – Reports are generated periodically and ad hoc. Customers can use their support.ca.com credentials to access private trust site which contains SLA details for the subscribed service

PPM – Performance data can be generated and reporting on in a self-service manner within the service. Currently no stock reports are available for this data. Real time system status is available at www.trust.ca.com

Microsoft Response:

The financial consequences are detailed in our response 8.10.2.

8.12.9

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

AWS Response:

Usage reports and historical performance data can be viewed via the Web, downloaded as text files, and accessed programmatically via API.

CA Response:

Agile and APIM – Reports are available upon customer request

ASM and PPM - Customers are sent monthly SLA reports

MAA - Reports are generated periodically and ad hoc. Customers can use their support.ca.com credentials to access private trust site which contains SLA details for the subscribed service

Microsoft Response:

This information is not available.

8.12.10

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

AWS Response:

On-demand IaaS and PaaS service deployment is supported 24x365.

CA Response:

N/A. CA only offers SaaS solutions and manages all aspects of the service. Clients do not have direct access to the environment.

Microsoft Response:

Access to the Azure Management Portal for deployment is available 24/7/365 from any device with internet access (Desktop, Laptop, Smartphone, and Tablet).

8.12.11

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

AWS Response:

Scale-up and scale-down of IaaS subcategory compute functionality, commonly known as Autoscaling, is available 24x365 via Web portal, CLI or API. Autoscaling is triggered by performance factors, scripting and applicable as either horizontal or vertical.

CA Response:

N/A. CA only offers SaaS solutions and manages all aspects of the service; monitoring and capacity planning is included as part of the service.

Microsoft Response:

Elasticity in Azure is available 24/7/365 via the Azure Management Portal.

8.13 Cloud Security Alliance

Describe your level disclosure of compliance with CSA Star Registry for each Cloud solutions offered.

- *Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5*
- *Completion of Exhibits 1 and 2 to Attachment B.*
- *Completion of a CSA STAR Attestation, Certification, or Assessment.*
- *Completion CSA STAR Continuous Monitoring.*

SHI Response:

The scope and requirements of this RFP are such that it would be impossible to include all of the cloud based offerings that SHI has in its catalog today. We will work to add products and solutions over the course of this contract as new technologies emerge or as customer needs arise.

SHI is responding today with offerings from AWS, Microsoft, and CA as well additional service offerings from our partner Ascent Innovations. For this Section each partner has provide a specific response.

AWS Response:

AWS is compliant with Level 1 CSA STAR Registry Self-Assessment. Please refer to AWS' self-assessment found within our Risk and Compliance Whitepaper, page 25-61. https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf. This is the latest CAIQ (v3) released by the CSA.

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

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

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

CA Response:

We have not performed a CSA assessment, however, CA has completed the CCM and CAIQ as part of Exhibit 1 and Exhibit 2 of this response.

Microsoft Response:

Please see Microsoft Azure CCM document for details on CSA compliance.

8.14 SERVICE PROVISIONING

8.14.1

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

SHI Response:

Should an emergency arise, each Purchasing Entity has access to a dedicated account team that will assist the customer to understand the emergency and assist in getting the best possible solution in a timely manner.

AWS Response:

SHI's IaaS and PaaS users will self-service their needs for implementation, and escalate to SHI for any issues. In response to escalations, SHI handles requests for IaaS and PaaS implementation with the same service SLAs described above. Depending on the extent of the implementation required, SHI will engage internal resources, AWS or other qualified subcontractors to meet the desired timeline.

CA Response:

Standard lead times for requests can be waived for requests that have a critical business need such as a data recovery effort.

Microsoft Response:

The customer has complete access to a majority of the features via the Azure Management Portal. For any additional features not covered the customer will work with the SHI Account Management Team and or Microsoft Account Team to expedite implementation requests.

8.14.2

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

AWS Response:

We help clients implement against any desired timelines with best-effort approach, and regularly see implementations requiring 2-6 week lead times for provisioning depending on complexity.

CA Response:

Services do not generally require client action for provisioning. General Service catalog requests, such as a data refresh, have a standard 48 hour lead time.

Microsoft Response:

The timeframe for provisioning of all services varies on the speed of the customers ISP and overall network access.

8.15 BACK UP AND DISASTER PLAN

8.15.2

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

AWS Response:

Please see response to 8.15.3.

CA Response:

Agile and APIM - The customer is responsible for the lifecycle of their data. We will retain all data until it has been deleted from our systems. We can remove data from our systems upon written request from the customer at termination of the contract.

ASM – Not available

MAA – Not available

PPM - Data and configurations can be retained indefinitely upon notification of a hold

Microsoft Response:

Azure Backup offers retention periods that are scheduled within the Azure Management Portal. The retention can be scheduled for up to 99 years.

8.15.3

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

AWS Response:

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

Availability

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

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

You should architect your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

Fault-Tolerant Design

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

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

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

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

As of this writing, there are twelve regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), South America (Sao Paulo), and China (Beijing).

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

Services (HHS) utilizing a FedRAMP accredited Third Party Assessment Organization (3PAO) for several AWS services.

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

CA Response:

CA Agile Central (Formerly Rally) - None - our DR plan is tested at a minimum semi-annually.

CA APIM - DR is provided only in a single geography at this point. Professional Services would need to be engaged to provide multi-geo DR

CA ASM – None

CA MAA – N/A

CA PPM - Risk of up to 24 hours of data loss

Microsoft Response:

Any potential issues are on a case by case basis. Solutions to any issues are offered via Azure MSDN Forums and Stack Overflow, both are manned by Microsoft MVP’s.

8.15.4

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

AWS Response:

See answer to 8.15.3

CA Response:

Agile Central (Formerly Rally) - We run a hot/warm data center configuration and have the ability to quickly failover if required. Our data centers are ~1300 miles apart to ensure redundancy. We perform full system planned switch over testing at a minimum semi-annually.

APIM - AWS datacenters provide redundancy and failover within a single AWS EC2 zone (i.e., a single geographic location). Professional Services would need to be engaged to provide multi-geo DR

ASM - ASM core services run in one primary data center, and can fail over to the DR site if there is a catastrophic failure.

MAA - MAA service is currently available from one data center only.

PPM - Business continuity plans are in place to restore production services from the nightly recovery point. Recovery is accomplished by deploying the service into the alternate data center within 72 hours

Microsoft Response:

All Azure Datacenters in the United States supports all of the stated features to run large scale applications. The Azure Status Site details each services available throughout all Azure Datacenters globally.

8.16 SOLUTION ADMINISTRATION

8.16.1

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

AWS Response:

Purchasing Entities have full control of user accounts, control over what those accounts can access, and any delegation or federation of such controls.

CA Response:

Agile and APIM - The customer is responsible for managing the lifecycle of all user accounts

ASM and MAA - The Purchasing Entity can manage their account and create sub-accounts within ASM.

PPM - User provisioning and authorization is fully self service via the web interface or available API's

Microsoft Response:

Identity and user accounts can be managed via the initial setup portal discussed in 8.19.2, role based access controls, and Azure Active Directory features.

8.16.2

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

AWS Response:

Purchasing Entities may install any anti-virus software and encrypt its data stores in whatever ways deemed fit for Low, Moderate and High Risk compliance requirements.

CA Response:

Agile - We have ClamAV installed on all Linux hosts and TrendMicro for Windows hosts.

APIM – AWS provides protection/virus scanning for data at rest

ASM, MAA, and PPM - Logical security is provided by ClamAV Antivirus.

Microsoft Response:

Azure offers several anti-virus options for their virtual machines. Microsoft, Symantec and TrendMicro are just a few of the offerings available via the Azure Marketplace. If applicable customer may use their existing anti-virus solutions in Azure provided the system requirements are met.

8.16.3

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

AWS Response:

Purchasing Entities are the owners of their data, and have full access to migrate data to other Cloud Hosting providers using industry standard techniques.

CA Response:

Agile - We can provide an export of data in XML and JSON formats

APIM – Data can be exported to accommodate relocation. A Professional Services engagement will be required.

ASM – REST API and raw data export (CSV).

MAA – Data can be provided upon request.

PPM – Self-service API's and defined dump files are available for migration efforts. See the response to 8.7.2 for details.

Microsoft Response:

Customer data stored in Azure can be removed at any time without assistance from Microsoft for the purposes of migrating or transferring to a successor cloud hosting solution provider.

8.16.4

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

AWS Response:

SHI can help Purchasing Entities create and manage user hierarchies, linked accounts, ACLs and other topologies so that they can support sophisticated scenarios for segregated access, access to data, visibility to metadata and chargeback requirements.

CA Response:

Agile - All administrative settings are configured by Subscription Administrators on a per subscription basis.

APIM – Delegated administration is built into the product

ASM – The ASM dashboard is accessible with any modern web browser with Internet access.

MAA – Designated Tenant Administrators from customer can administer the service for their user-base from any supported browser.

PPM – Assignment of administration rights is self-service. The client can define multiple user accounts to manage the service

Microsoft Response:

Access can be offered to participating entities using the information from the responses in 8.16.1 and 8.19.2.

8.16.5

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

AWS Response:

Purchasing Entities can use a number of subcategory services such as SAML, SSO, Active Directory and other technologies to manage participating entities' access to IaaS and PaaS services.

CA Response:

Agile - Subscription Administrators have the ability to configured subscription settings.

APIM – The product allows for a number of areas that can be configured/policies to be created for purposes of managing the solution

ASM and MAA – Not applicable

PPM – Process flows and service configuration can be partitioned per client defined entity allowing for entity specific management. See PPM SaaS User's Guides for detailed description of this functionality.

Microsoft Response:

Please see the responses to questions 8.16.1 and 8.19.2.

8.17 HOSTING AND PROVISIONING

8.17.1

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

AWS Response:

The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS regions and lets customers provision resources across multiple regions.

Command Line Interface

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

Use Existing Management Tools

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

- AWS Management Portal for vCenter enables customers to manage their AWS resources using VMware vCenter. The portal installs as a vCenter plug-in within the existing vCenter environment. Once installed, it enables customers to migrate VMware VMs to Amazon EC2 and manage AWS resources from within vCenter. The AWS resources that customers create using the portal can be located in their AWS account, even though those resources have been created using vCenter. For experienced VMware administrators, AWS Management Portal for vCenter provides a familiar look and feel that can make it easy to start using AWS. AWS Management Portal for vCenter is available at no additional charge.
- The Amazon EC2 VM Import Connector extends the capabilities of VMware vCenter to provide a familiar graphical user interface customers can use to import their preexisting Virtual Machines (VMs) to Amazon EC2. Using the connector, importing a VM is as simple as selecting a VM from the vSphere infrastructure, and specifying the AWS region, Availability Zone, operating system, instance size, security group, and Amazon Virtual Private Cloud (Amazon VPC) details (if desired) into which the VM should be imported. Once the VM has been imported, customers can launch it as an instance from the AWS Management Console and immediately take advantage of all the features of Amazon EC2.

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

CA Response:

Agile - All new systems should be provisions according to our baseline standards and we use configuration management tools to ensure all systems are created with the same standards.

APIM – CA SaaS Ops has a well-defined Service Introduction and update process, including review boards, staged rollouts and follow-ups to ensure service integrity. Our cloud provisioning stack is tied to AWS EC2 services, and includes S3 and RDS for storage; RHEL instances for the applications; route 53 DNS services; cloud front for monitoring; and ELB for load balancing

ASM and MAA– Automation tools are used to install and configure ASM software on CA infrastructure. SOP documents are used by CA internally.

PPM – Workstation requirements are documented in release notes.

Microsoft Response:

Provisioning in Azure can be best accomplished with the use of Azure Resource Managers. There's several advantages that ARM provides over the existing Azure Service Management (ASM) API, including simplifying complex configurations, repeatable deployments via declarative templates, resource tagging, role-based access control (RBAC) and more.

8.17.2

Provide tool sets at minimum for:

- ***Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)***
- ***Creating and storing server images for future multiple deployments***
- ***Securing additional storage space***
- ***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).***

AWS Response:

Please see the response to question 8.17.1

CA Response:

Agile - We utilize configuration management tools to ensure consistent configuration across our servers. We have redundant systems for all critical infrastructure and have the ability to add additional storage if deemed necessary. Access to monitoring tools is provisions according to the principle of least privilege and is only granted based upon business need.

APIM – Servers are brought up on demand. AWS EC2 storage is elastic, and can be expanded on demand. All SaaS based instances are monitored by CA SaaS Ops. With Hybrid deployments, customers can manage the on premise components of the deployment using their own tooling or CA products.

ASM – See response to 8.17.1. Additional storage is added manually. ASM uses Nimsoft Monitor, third-party open source monitoring tools, and ASM itself to monitor the health of ASM internal services and servers.

MAA – See Response to 8.17.1. Virtual storage can be added when needed. MAA is monitored internally as well as externally using multiple tools recognized within industry.

PPM – Deploying and creating new servers is not applicable. Additional storage space - Dynamically allocated NAS. Monitoring tools is real time availability metrics at www.trust.ca.com

Microsoft Response:

Azure Virtual Machines lets you deploy a wide range of computing solutions in an agile way. Deploy a virtual machine nearly instantly, and pay by the minute. With support for Microsoft Windows, Linux, Microsoft SQL Server, Oracle, IBM, SAP, and Azure BizTalk Services, you can deploy any workload and any language on nearly any operating system.

Azure Storage provides the flexibility and hyper-scale needed to store and retrieve large amounts of data. Use Azure Blob Storage (Object Storage) to store unstructured data, such as documents and media files. Use Azure Table Storage for structured NoSQL data. Use Azure Queue Storage to reliably store messages. And use SMB-based Azure File Storage for existing or new applications—no code changes are required.

You can monitor key performance metrics for your cloud services in the Azure classic portal. You can set the level of monitoring to minimal and verbose for each service role, and can customize the monitoring displays. Verbose monitoring data is stored in a storage account, which you can access outside the portal.

Monitoring displays in the Azure classic portal are highly configurable. You can choose the metrics you want to monitor in the metrics list on the **Monitor** page, and you can choose which metrics to plot in metrics charts on the **Monitor** page and the dashboard.

8.17.3

Ability to provide IaaS, PaaS, and SaaS solutions as defined service offerings with established rate structures

AWS Response:

See response to 8.17.1

CA Response:

Only SaaS services are provided. Standard, per user subscription rates are provided.

Microsoft Response:

IaaS, PaaS and SaaS based services in Azure have individualized pricing that is available when selecting those services via the Azure Management Portal.

8.18 TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)

8.18.1

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

AWS Response:

A free-tier IaaS service level is offered for clients to try its subcategory services. Services ordered beyond the free-tier are billed at published rates based on consumption. Clients only pay for what they consume and services can quickly be decommissioned to prevent further billing.

CA Response:

Agile - CA offers its clients a trial period and training can be included as a service.

APIM – CA Professional Services and CA Education offer packaged training and service introduction courses that can be tailored to each customers' needs. Typical offerings include:

A standard five day deployment and training package is available for purchase and includes:

- Portal - trains SaaS APIM users (covering CMS content creation; site branding; user creation; API publication; application creation; interactive API documentation creation; and more)
- Policy Manager – introduction to the Gateway and policy creation
- Quick Start – help with implementing the Portal to reflect the customers' brand and API management initiative (includes tips and techniques on CSS editing; API publication; API security; WADL/Swagger creation, and more)

ASM – 30-day trial accounts are available at no cost.

MAA – Customers can self-subscribe to trial environment to try out the product for free.

PPM – No trial periods are available. CA Technologies has a full catalog of web based and instructor lead training for PPM SaaS.

Microsoft Response:

Azure has the capability of both staging and production environments for the services offered. Environments can be created via Azure credits provided through all MSDN subscriptions in addition to the Azure DevTest Labs feature which is now in preview.

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.

AWS Response:

SHI would address any outstanding questions and provide needed documentation, and also work in good faith to assist evaluating entities' verification of service utility on an as-needed basis.

CA Response:

CA offers trial environment for interested customers to evaluate the product before making a purchase. For paying customers, CA also offers a non-production environment for testing any functionality prior to rolling out to users.

Microsoft Response:

A proof of concept can be provided with the services provided in 8.18.1. Additional services to support a proof of concept would be provided on a case by case basis.

8.18.3

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

AWS Response:

The support described above is offered at no additional cost.   Training offered at no cost consists of a vast online library of CBT, whitepapers, User and Administration guides, as well as online subject matter discussions.

CA Response:

CA Support is CA Technologies standard support maintenance that offers multiple access methods and support services to meet your operational support and business needs, including:

- Online support for self-service and case management
- 24x7 telephone support for Severity 1 cases via a single telephone number (by country)
- Product release, version and certification updates
- Product fixes and alerts for high impact problems and fixes
- Troubleshooting
- Multi-platform and product integration support
- Implementation and upgrade project support
- Access to knowledge documents, product compatibility information and documentation
- Access to CA Technologies programs such as: Go Live with CA Technologies; CA Communities; CA Beta Programs; CA Green Books; and CA Tech Insider e-newsletters

Support is included in the maintenance cost and all Training must be purchased at additional cost.

Microsoft Response:

Value added support and training are offered by Microsoft Virtual Academy, Channel 9 and TechNet Virtual Labs. Microsoft Learning Partners provide in person trainings at facilities nationwide. The Microsoft Ignite Conference also provides this level of training as well.

8.19 Integration And Customization

8.19.1

Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

AWS Response:

Our IaaS and PaaS services are fully documented and ready to integrate into third party applications via REST APIs, CLI, and shell scripting.

CA Response:

Agile - There are various integrations available between the Agile Central and other platforms. All supported integrations can be found here: https://www.rallydev.com/product-feature/rally-platform-integrations-overview.

APIM – The SaaS Portal features a set of public, documented APIs for integration with third parties

ASM – ASM has a REST API that can be used to interact with ASM programmatically. Nimsoft Monitor has a plug-in module for integration with ASM.

MAA – MAA SDK can be utilized to integrate it with other products. CA Services can be engaged for such implementations.

PPM – Standard API's are provided for integration development. Additional details are provided in the user documentation.

Microsoft Response:

Azure has connections to over 3000 SaaS based apps covering virtual machines, developer services, API applications, Azure Active Directory application connectors, Web applications, data services and Microsoft Dynamics solutions online via the Azure Marketplace.

8.19.2

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

AWS Response:

Purchasing Entities can fully customize and personalize our IaaS and PaaS services to support their specific needs via REST APIs, CLI, and shell scripting.

CA Response:

Agile - We offer a RESTful API that can be used to create integration services not offered.

APIM – SaaS Portal offers a number of ways to customize, configure and brand the product to suit each customer's needs

ASM – ASM Public Status Pages can be branded. The REST API can be used to develop customized applications.

MAA – MAA SDK can be utilized for customizations. Many personalization options are available out of the box. CA Services can be engaged for custom requirements.

PPM – CA PPM SaaS is highly configurable to enable client specific processes. Both the UI and workflows can be configured.

Microsoft Response:

To initially administer your Microsoft Azure services under your Enrollment, there are four distinct administrative roles: the Enterprise Administrator, The Department Administrator, the Account Owner and the Service Administrator. Users are required to authenticate using a valid Microsoft Account (LiveID http://signup.live.com) or School or Work Account (Azure-based Active Directory). Please ensure the ID entered is associated with a monitored mailbox as enrollment and account notifications will be sent to this mailbox.

The roles complete tasks on three different Microsoft Azure portals. The Enterprise Portal, the Account Portal and the Management Portal.

- **Enterprise Administrator**
  The Enterprise Administrator has the ability to add or associate Accounts to the Enrollment, can view usage data across all Accounts, can view the monetary commitment balance associated to the Enrollment with pricing data from the partner. There is no limit to the number of Enterprise Administrators on an Enrollment.

- **Account Owner**
  The Account Owner can add Subscriptions for their Account, update the Service Administrator and Co-Administrator for an individual Subscription, view usage data for their Account, and view Account charges if the Enterprise Administrator has provided access. The Account Owner will not have visibility of the monetary commitment balance unless they also have Enterprise Administrator rights.
- **Service Administrator**
  The Service Administrator and up to nine Co-Administrators per Subscription have the ability to access and manage Subscriptions and development projects within the Azure Management Portal. The Service Administrator does not have access to the Enterprise Portal unless they also have one of the other two roles.

8.20 Marketing Plan

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

SHI Response:

SHI understands that when implementing this contract, it will be important to communicate with NASPO ValuePoint and with each Participating State to ensure that our messaging to Participating Entities is accurate and timely. We recognize that we will need to understand NASPO ValuePoint's vision for the contract and the unique requirements of each State, and that we will then need to market the benefits of the contract to each eligible agency, city, county, township, school district and higher education institution.

In addition, SHI plans to build on the experience we've gained from the NASPO ValuePoint SVAR contract to help make this contract successful for the Participating Entities.

SHI has designed a preliminary marketing plan for the contract to ensure maximum participation. We will work with the individual states on appropriate timing, and agree upon appropriate venues for any face-to-face marketing initiatives. SHI's implementation/transition plan for the new contract provides for a smooth and seamless experience for the States included in the NASPO ValuePoint Cloud Solutions agreement, whether we have worked with these States under another NASPO ValuePoint contract or they are new to SHI.

SHI's marketing or outreach to all the participating entities on the contracts we hold is a multi-prong approach:

- SHI's CRM System has been uploaded with every public entity within each State. Each State's Account Executives establish a relationship with each purchasing agent/buyer and IT administrator within the organization and update our CRM so that we can verify that they have been reached. The SHI Account Executive discusses the contract with them and provides them with contact information, website information, and contract guidelines for working with SHI. SHI's Account Executives are proactive in their approach with our customers and prospects, and they regularly engage in on-site meetings and joint phone calls with our publisher representatives.

- SHI's Inside Sales Team members walk individual customers through our www.shi.com website where customers can create quotes, purchase items, obtain order status, and generate reports of their purchases.
- SHI's marketing team subscribes our new CRM contacts to SHI's monthly newsletter, which contains helpful information on SHI's publishers, new products and promotions, changes to programs, and industry news.
- SHI participates in statewide and local vendor events. SHI Account Executives and publisher partners will meet with all available entities and discuss SHI's support plan and our cloud partners' solutions.
- SHI works with each State to create timely and meaningful Tech Days for individual state and local entities to attend to learn about new cloud solutions for their IT environments.

Each of these elements come together to ensure that SHI is effectively marketing the new Cloud Solutions contract.

8.21 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.

SHI Response:

SHI can offer Professional Services towards application development and migration, scale or complex designs and implementations, 24x7x365 helpdesk, Backup and DR, server patching, monitoring and full-service NOC, billing and financing, split billing and chargeback management, optimization management, and other lifecycle services.

As part of this response we have included an attachment about Office 365 JumpStart, which is available from SHI.

SHI is also pleased to provide a response from our partner Ascent Innovations.

Ascent Innovations

Ascent Innovations, is a Microsoft Dynamics certified solution provider for mid to large size companies, government and education organizations. Ascent Innovations was founded as a firm in 2009 with the goal of providing customer-focused enterprise solutions and high quality service. Now, it has a combined staff experience of decades in ERP/CRM/Cloud Azure deployments.

Ascent Innovations is a Microsoft Dynamics ERP/CRM/Cloud Azure certified partner, specializing in complex implementations and is fully capable of provisioning for the Microsoft Azure Cloud services to be recommended by our Prime supplier, SHI,Inc.

Ascent Innovations is owned and managed by Sohena Hafiz, and being a financially sound and minority-woman owned and growing company, has received five government small business certifications. Certifications provided by the Federal Small Business Administration as an 8(a) firm, the State of Illinois' BEP program, the Cook County WBE/MBE certification, the City of Chicago WBE certification and the WBENC certification.

The Federal Small Business Administration 8(a) certification, to be utilized as the primary certification, is valid through May of 2023. Thus providing a woman owned/minority owned status that can be utilized by *NASPO* through the life of the sourcing agreement.

Ascent Innovations possesses the expertise and depth as a Microsoft Dynamics ERP/CRM/Azure certified partner, specializing in Dynamics AX, GP, CRM, SQL Server, SharePoint with a focus on Education, Public Sector, Manufacturing, Professional Services customers, with emphasis on Financial Management, Project Accounting, Business Analytics, Supply Chain, Service Management, Fixed Assets and Compliance within a Cloud/Hosted environment.

We have demonstrated expertise in building integrations with Dynamics ERP/CRM on Azure platforms with various external systems, to include EDI, RF solutions, Mobile apps, BI tools, Data Integration tools, Inventory/3PL systems, payment gateways, logistics, electronic document management, e-Commerce sites, etc. Additionally, we have enhanced the operations by building reports for staff, managers and executives, using SSRS, MR, SSAS, Role Centers, etc.

Ascent Innovations is a certified partner with multiple 3rd party software providers for Microsoft Dynamics products, including BlackLine, DataMasons EDI, RF Smart, Solver BI360, Scribe, M4 AGL, KwikTag, Dynamics Anywhere, eOne Solutions, etc.

Ascent Innovations' Microsoft Cloud/Azure Product services offering:

Ascent Innovations is able to deploy functional and technical consultants for the Microsoft Cloud/Azure environment. Our capabilities and skills are provided through on-site and/or remotely located for the full suite of Microsoft offerings within the Azure environment. Providing complete deployment services allowing the NASPO customer to make a solution choice and deploy in full production mode. The following are areas Ascent Innovations focuses for its customers:

Microsoft Azure

Do more, spend less with Microsoft Azure. With the fast pace of innovation constantly accelerating, it's becoming increasingly expensive to keep investing in the latest and greatest IT solutions. At the same time, relying on older solutions while your competitors invest in new ones gives them a leg up on you to anticipate, manage, and respond more quickly to change. You want to focus on running your organization and the bottom line, not your technology infrastructure. With Microsoft Azure, you can build, deploy, and manage applications in the cloud without worrying about the cost of purchasing new server hardware. You can easily scale up or down as needed and gain peace of mind knowing your data is safe, secured and protected by Microsoft-managed datacenters.

Enterprise Mobility Suite

Simplify security and stay productive with the Microsoft Enterprise Mobility Suite (EMS). EMS includes Azure Active Directory, Azure Rights Management, Microsoft Intune, and Advanced Threat Analytics to provide organizations with cost-effective, comprehensive security for users, devices, applications, and data. Organizations are struggling to meet the challenges posed by the influx of consumer-oriented technology into the workplace, which is eroding standards-based approach to IT, and by the growing expectation of users to access all of their work resources from any location, on any device and at any time.

The Enterprise Mobility Suite (EMS) is designed to help organizations meet these challenges by providing a people-centric IT solution that gives users access to corporate resources from the devices of their choice, while making it easier for IT administrators to securely manage devices, data, and applications across platforms.

Managed Services

Staying on top of technology trends has become increasingly expensive. With our deep understanding of Cloud deployment together with our expertise in Cloud based IT infrastructure we can design unique solutions that make technology your trusted investment.

Let Ascent Innovations help your organization:

- Transition to a cloud environment or extend the value of existing IT investment
- Scale out quickly and affordably by running apps and workloads in the cloud
- Boost productivity and collaboration with SharePoint Online.
- Work with full versions of Office anytime, anywhere, and on virtually any device with Office 365
- Implement flexible, affordable data backup and disaster recovery solutions by taking advantage of cloud services like Microsoft Azure
- Safeguard organizational data by integrating enterprise identity management solutions like Active Directory with cloud services

Office 365

Office 365 keeps itself up to date, so you always have the latest features of Word, Excel, PowerPoint, and more.

Office Applications - Office 365 provides applications you're familiar with and files that are always accessible, always up to date. So online or off, at your desk or on the go, from your PC/Mac or your iOS, Android™, or Windows device, you can get to what you need, when and where you need it.

Email & Calendar - Office 365 synchronizes emails, calendars, and contact information across your devices in real time. So you have the latest information, no matter what device is in your hand.

Online Meetings - It's easy to meet and connect online from wherever you are on whatever device works best. HD video puts you—and up to 250 people—all at the same table. It's a smart way to share information and meet colleagues from multiple locations.

File Sharing -With 1 TB of personal document storage, having your files stored online makes it easy to store, organize, and share them, so you can work on documents with teammates, share reports with organization partners, or connect with constituents. Your files are always up to date, so everyone has access to the latest version.

Video Management - Office 365 Video gives you a scalable enterprise video solution. It allows employees to find, discover, and view important topics and ideas across the organization—across their devices—staying informed and in unison.

Windows 10

Windows 10 is designed for the modern world of cloud services and mobility simply put Windows 10 is simple to use.

Windows 10 integrates the Cloud with the PC, delivering fully-functional devices that can operate web-apps, browsing, Windows Store apps, Windows desktop apps, you name it. It also integrates seamlessly with other 3rd party Cloud solutions like CRM, E-Commerce, ERP and Inventory, just to name a few.

Cloud synchronization is key with Windows 10. Not only can users synchronize their account, preferences, favorites, settings, and apps between devices using their Microsoft or Office 365 account, they will have the ability to sync their files using OneDrive Cloud storage or email, calendar and contacts with Outlook.com.

Windows 10 is still Windows, enabling the best devices for powerful, general-purpose computing. You can run new modern Windows Store apps, desktop apps that run on Windows 7 and later, and of course the custom apps or programs you have invested in for your organization.

Windows doesn’t need to be always connected to be functional. Users can work with locally installed apps and save those files critical to their workflow on a local drive – and then be confident they will sync back to the cloud when they’re connected again.

SharePoint

SharePoint Products and Technologies provide enterprise-scale capabilities to meet organization-critical needs such as managing content and enterprise processes, simplifying how people find and share information across boundaries, and helping to enable more informed decision-making.

Many organizations use SharePoint to create websites. It can also be used as a secure place to store, organize, share, and access information from almost any device. All you need is a web browser, such as Internet Explorer, Chrome, or Firefox.

SharePoint is a cloud-based service, hosted by Microsoft, and is for organizations of all sizes. Instead of installing and deploying SharePoint Server on-premises, a decision maker can subscribe to an Office 365 plan or to the standalone SharePoint Online service. Your employees can create sites to share documents and information with colleagues, partners, and customers.

Ascent Innovations Microsoft Cloud/Azure Technology Services Offerings

Technical Consulting and Architecture Services

- Ascent Innovations provides technology expertise during engagements to facility a full solution, aligning with the *NASPO* customer’s need.
- The Ascent Innovations’ solution architect provides for design and delivery for Data Storage, Server design, Operating Systems, Virtualization, Email, Identity Management, Disaster Recovery and timely Backups.

Strategic Planning Services

- Ascent Innovations has staff and experience to help *NASPO’s* customers to plan for the changes and variables that will confront them within their IT deployment utilizations and environments. We will sit down with decision makers and define a course for managing tomorrow’s needs and direction.

Network and Service Architect Assessments

- The Ascent Innovations has the experience to simplify the limitless choices that are available today.
- We will facilitate discussions and lead the customer through the necessary Joint Application Discovery (JAD) sessions, beneficial for an early development of a highly valued direction/roadmap.

Security Planning Services

Ascent Innovations will provide services within a Microsoft Azure Cloud environment to protect against:

- Spyware and malware
- Data Interception
- Identity theft
- Viruses
- Hacking attempts

Standard best practice for security is given the primary importance to include:

- Acceptance of industry/organizational standards
- System development and maintenance
- Organizational continuity planning
- Compliance and Governance

Training Services to End Users

- Ascent Innovations is staffed with fully qualified trainers
- Providing remote and onsite learning experience – through Webinars and In-person training.
- We provide Cloud and Virtualization training, certifications and solutions customized to the NASPO sourcing community. Ensuring the realization of Return on Investment for IT decisions and expenditures.

Ascent Innovations is included within the SHI, Inc response to the NASPO Cloud Storage and Productivity Services request. Ascent Innovations recognizes the importance of our service offerings for technology choices of the NASPO customer community.

We believe our dedication, knowledge, skill sets and unique coverage for the services of the Microsoft Azure platform will allow SHI and Ascent Innovations to create and foster a successful, efficient and best value offering for a Premier Cooperative Purchase Service for Education as requested by NASPO.

CA Response:

Professional Services might be engaged in the following ways:

- Architecture Consulting – consulting on the creation of a VPN integration between the Portal service and the customer's on premise/datacenter-located APIs
- CMS Customization – we provide a number of common Adobe CQ resources out of the box, but PS might be engaged to create new templates, layouts and other components in Adobe CQ. These would then be given to the Ops team who will apply the change to the Adobe CQ CRX for that specific tenant (i.e., the customization would only be available for the paying customer; would not be available for other tenants)

- Gateway Policy Creation – creation of Gateway policies, such as:
  - Create encapsulated assertions that implement a customer's specific security requirements (as well as other business requirements) and will be available as a Policy Template in the Portal when an API Owner goes to publish their APIs
  - Create custom policies to integrate the SaaS-based API Management imitative back into the customer's enterprise resources in a secure manner, or a to a third party/cloud-based resource
- General API Management Consulting – helping the customer apply their branding to the Portal; create Account Plans; onboard users; publish APIs, etc and then migrate everything from non-Production to Production

8.22 Supporting Infrastructure

8.22.1

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

AWS Response:

At a minimum customer needs to have access to the internet.

CA Response:

Agile - An internet connection and supported web browser are required to utilize the stock service.

APIM – For SaaS: a desktop PC or laptop able to run a browser (portal) and 64-bit application (interface to the Gateway component)

For Hybrid: a 64-bit server with 4-16 cores; 8-64GB of RAM and 20-100+ GB of storage space, depending on the volume of transactions expected

ASM - No infrastructure is required unless the Purchasing Entity decides to deploy ASM on-premise monitoring stations, in which case they will need to deploy at least one physical or virtual machine.

MAA – No infrastructure is required unless the Purchasing Entity decides to deploy MAA on-premise cloud connect agent to integrate any of the on-premise user stores, in which case they will need to deploy at least one physical or virtual machine.

PPM – An internet connection and supported web browser are required to utilize the stock service.

Microsoft Response:

Please see the response to question 8.3.5 for minimum infrastructure requirements. Additional infrastructure requirements can be discussed on a case by case basis.

8.22.2

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

AWS Response:

SHI will seek POs from Purchasing Entities to cover costs for infrastructure deployment and any requisite services needed as identified and approved by Purchasing Entity decision makers.

CA Response:

Agile - Deployment of the service is included in the base offering and is the responsibility of CA Technologies.

APIM – Customer will bear the costs; CA Professional services can help with installation

ASM – If an (optional) ASM on-premise monitoring station is needed by the Purchasing Entity they will incur those costs.

MAA – If an (optional) MAA on-premise cloud connect agent is needed by the Purchasing Entity, they will incur those costs.

PPM – Deployment of the service is included in the base offering and is the responsibility of CA Technologies.

Microsoft Response:

Installation of new infrastructure can be completed by SHI unless otherwise agreed upon by both parties. NASPO would incur all costs of said installation.

8.23 Alignment Of Cloud Computing Reference Architecture

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

AWS Response:

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

CA Response:

Agile - Only SaaS is being offered via a public cloud.

APIM – The SaaS portal runs in Amazon Web Services. For an overview of how AWS conforms to NIST, please refer to: https://aws.amazon.com/about-aws/whats-new/2016/01/nist-800-53-standardized-architecture-on-the-aws-cloud-quick-start-reference-deployment/

ASM - As a monitoring service, ASM is considered to be SaaS product.

MAA – MAA is considered a SaaS product.

PPM – PPM is considered a SaaS product.

Microsoft Response:

The cloud architecture presented will be based on NIST determined architecture in order to offer best practices cloud practices that remains compliant with the customers' requirements.

9 CONFIDENTIAL, PROTECTED OR PROPRIETARY INFORMATION

SHI does not have any Confidential, Protected, or Proprietary information in this response.

10 Exceptions and/or Additions to the Standard Terms and Conditions

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

SHI Response:

Per bid instructions SHI is including the requested clarifications to the Master Agreement Terms and Conditions. These clarifications also include:

- Response to terms from Microsoft
- AWS Access Agreement

Upon award, SHI agrees to work with NASPO ValuePoint on the review and final agreement of terms and conditions associated with this response. The primary point of contact for these discussions will be:

Natalie Slowick
Natalie_slowick@shi.com
732-868-5902

11 COST PROPOSAL

Per bid instructions, SHI has completed Attachment G – Cost Proposal and we have included it as a separate document from the Technical Response.

12 ADDITIONAL INFORMATION

Immediately following is some additional information that SHI has included as part of our response.

Microsoft Office 365 Jumpstart

Statement of Work

OVERVIEW

Supported by a winning combination of SHI's Licensing Team, Professional Services Organization (PSO), and Microsoft's FastTrack Center (FTC), customer will be guided through an overview of Office 365, creation of a success plan and key initial onboarding steps, all designed for a seamless handoff to Microsoft's FTC for completion of the onboarding process.

DELIVERABLES

- Creation of pilot tenant for testing, if requested
- Comprehensive tour of your new Office 365 tenant
- Creation of success plan to help facilitate the onboarding process
- Q&A with an SHI Solution Architect
- Activate, setup and configure tenant and test client
- Set up all administrative accounts needed by the client
- Walkthrough of administrative portal
- Add clients primary domain in the tenant and verify ownership
- Configure DNS for Skype for Business Online if Skype for Business on-premise is not currently in the environment
- Identify SSL requirements

RESOURCES AND SKILLS

SHI Onboarding Support

- SHI will provide a ***Cloud Onboarding Support Specialist***, responsible for managing the customer and onboarding process through to the Microsoft FastTrack center.
- SHI will provide an ***Onboarding Solution Architect(s)***, responsible for onboarding technical activities including providing CORE onboarding services and answering CORE onboarding questions.

ASSUMPTIONS

- SHI is not responsible for lost data. SHI recommends that the customer perform a full working backup of their data prior to the commencement of services.
- SHI is not responsible for delays caused by failures; including but not exclusive to Microsoft licensing, systems, personnel, environmental causes or in receiving data from the customer.
- The customer will make the necessary administrative usernames and passwords available to the SHI consultants.

ASSUMPTIONS *(CONT.)*

- The customer will provide detailed and accurate information regarding their current network environment. This information will include the technical configuration of the domain environment.
- All hardware and/or software and licensing required to perform the above services will be provided by and is the responsibility of the customer.
- The customer will provide a technical point of contact during the time of this project.
- All parties agree that personnel shall not be asked to perform, nor volunteer to perform, engineering and/or consulting tasks that lie outside the skill sets and experience of personnel. Personnel have the right to decline on a service request if the request falls outside the scope of their experience and expertise.

CUSTOMER RESPONSIBILITIES

The customer and SHI are responsible for the successful execution of this project. The customer agrees to the following:

- Prior to the start of Office 365 Jumpstart, the customer needs to return the signed SOW. All Project communications will be addressed to the customer specified point of contact ("Customer Contact").
- The Customer Contact shall have the authority to resolve conflicting requirements.
- The Customer Contact will ensure that any communication between the customer and SHI is made through SHI's Cloud Onboarding Support Specialist.
- The Customer Contact will provide technical points-of-contact ("Technical Contacts"), who have a working knowledge of the enterprise components to be considered during this project. SHI may request that meetings be scheduled with Technical Contacts.
- The customer will inform SHI of all access issues and security measures, and provide access to all necessary systems as required.
- The customer will provide, at no expense to SHI: computer hardware, software, and access to the customer network as required to complete the work described in this Statement of Work.
- The customer agrees that all related information regarding this project will be communicated to SHI as expeditiously as possible.

CONTINUED ON PAGE 2

CUSTOMER RESPONSIBILITIES *(CONT.)*

The customer will provide individual resources outlined below to be participants for this project effort. These resources will participate in all required steps and will be fully or partially responsible for tasks and deliverables where appropriate:

Resource	Role
Sponsor/Project Manager	Project and resource coordination to support the effort as well as authority to make decisions and acceptance at project completion.
IT Resource	Provide building access, workspace access, and general IT requests related to the effort. May also have responsibility for network, data center and project team activities.

PROJECT SCOPE

Service Description	Details
90-minute Kickoff	We will conduct a 90-minute kickoff call to review the Office 365 portal, develop a deployment plan, create a pilot tenant (if necessary), and review the onboarding process.
Schedule a Jumpstart	As a follow-up to the kickoff call, we will schedule a jumpstart call (up to four hours) to set up basic configuration tasks and familiarize you with your new Office 365 tenant.
Microsoft FastTrack Center Project Management	Upon completion of the jumpstart, we will work on your behalf to manage the logistics with the Microsoft FTC to help you take advantage of the benefits offered to Office 365 customers. This includes continued CORE onboarding services in addition to service onboarding for additional Office 365 workloads if desired.
Total Value of Service	SHI will provide these services, valued at $893.00, at no cost.

TERMS AND CONDITIONS

The customer agrees to add SHI as the Partner of Record for Office 365 workloads that are part of the onboarding services provided under this SOW.

SOW ACCEPTANCE

The project Terms and Conditions are as outlined in this document. Once fully executed, this document will become the Statement of Work for the project defined in this document. The customer's signature below authorizes SHI to begin the services described above and indicates the customer's agreement to process and pay the invoices associated with these services.

CUSTOMER ACCEPTANCE

SHI International Corp			
SHI Contact Name			
SHI Signature		**Agreement Date**	
Customer			
Contact Name/ Title		**Company**	
Services Address			
Customer Signature		**Signature Date**	

ATTACHMENT E

Service Provider Terms and Conditions

ATTACHMENT E-1

Microsoft Additional Use Rights and Restrictions

Additional Use Rights and Restrictions

These Additional Use Rights and Restrictions shall apply to each Enterprise's use of Products

____

1. General.

Right to use. Purchasing Entity may access and use In-Scope Services, and install and use a Client (if any) included with its Subscription, only as described in this agreement. All other rights are reserved.

Acceptable use. Purchasing Entity will use In-Scope Services only per the AUP. Purchasing Entity will not use In-Scope Services in any way that infringes a third party's patent, copyright, or trademark or misappropriates its trade secret. Purchasing Entity may not reverse engineer, decompile, work around technical limits in, or disassemble In-Scope Services, except if applicable law permits despite this limit. Purchasing Entity may not rent, lease, lend, resell, transfer, or host In-Scope Services to or for third parties.

Compliance.

Purchasing Entity will comply with all laws and regulations applicable to its use of In-Scope Services.

In providing In-Scope Services, Contractor and Microsoft will comply with all laws and regulations (including applicable security breach notification law) that generally apply to IT service providers. Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry or government function that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Purchasing Entity will obtain any consents required: (1) to allow it to access, monitor, use, and disclose user data; and (2) for Contractor and Microsoft to provide the In-Scope Services. If Purchasing Entity is an educational institution, it will obtain any parental consent for end users' use of In-Scope Services as required by applicable law.

Customer Data. Customer Data is used only to provide Purchasing Entity In-Scope Services. This use may include troubleshooting to prevent, find and fix problems with those In-Scope Services' operation. It may also include improving features for finding and protecting against threats to users. Neither Contractor nor Microsoft will derive information from Customer Data for any advertising or other commercial purposes. As between the parties, the Purchasing Entity retains all right, title and interest in and to Customer Data. Neither Contractor nor Microsoft acquires rights in Customer Data, other than the rights Purchasing Entity grants to Microsoft through Contractor to provide the Online Services to Purchasing Entity. This paragraph does not affect Microsoft's rights in software or Online Services Contractor and Microsoft license to Purchasing Entity.

Contractor and Microsoft will enable Purchasing Entity to keep Customer Data in DPT Services separate from Microsoft's consumer services.

Customer Data will not be disclosed unless required by law or allowed by this agreement. Purchasing Entity's contact information may be provided so that a requestor can contact it. If law requires disclosure, Contractor and Microsoft will use commercially reasonable efforts to notify Purchasing Entity, if permitted.

Customer Data may be transferred to, and stored and processed in, any country Contractor or Microsoft maintain facilities, except when a tenant for DPT Services is provisioned in the United States, in which case Customer Content shall be processed and stored at rest in the Continental United States.

Security Incident Notification for DPT Services. Solely for DPT Services, the following terms and conditions apply:

If Microsoft becomes aware of any Security Incident (as defined herein), Microsoft will promptly (1) notify Purchasing Entity of the Security Incident; (2) investigate the Security Incident and provide Purchasing Entity with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Purchasing Entity's administrators by any means Microsoft selects, including via email. It is Purchasing Entity's sole responsibility to ensure Purchasing Entity's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Purchasing Entity must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to an Online Service.

5-day Security Incident notification for Government Community Cloud Services. As an exception to the foregoing, notification of Security Incident solely pertaining to Government Community Cloud Services will be delivered within 5 days after Microsoft determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, Purchasing Entity must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);

2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:

   a. Name;

   b. Title;

   c. Email address registered as an administrator on the Online Services;

   d. Email address not registered as a user on the Online Services;

3) Name of Purchasing Entity;

4) Enrollment number (provided by Contractor and assigned by Microsoft) to represent Purchasing Entity's Tenant or Azure Subscription, on Contractor's subcontract with Microsoft.

Microsoft expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Microsoft, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Reimbursement of Security Incident Remediation Costs. To the extent that a Security Incident for a DPT Service results from Microsoft's failure to comply with its obligations under the Master Agreement (and, where applicable, Participating Addenda), and subject to the Limitation of Liability section in this Agreement, Microsoft will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Microsoft's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Microsoft under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in the Limitation of Liability section.

Changes. In-Scope Services may be changed periodically. As such, Purchasing Entity's use of them will be subject to a revised OST, then-current as of the date it renews its subscription. For In-Scope Services that include client software, Purchasing Entity may be required to run a client software upgrade on its devices after a change to maintain full functionality, in accordance with the terms and conditions of the OST.

Use rights. Use rights specific to each In-Scope Service are posted online at the link to the OST, which is hereby incorporated by reference into this agreement

Confidentiality and Security.

For DPT Services, Contractor and Microsoft will (a) implement and maintain all appropriate administrative, physical, technical, procedural safeguards and organizational measures, internal controls, and data security routines intended to protect Customer Data against accidental loss or change, unauthorized disclosure or access, unlawful destruction, hacks, introduction of viruses, disabling devices, malware, and other forms of malicious or inadvertent acts that can disrupt Purchasing Entity's access to its Customer Data; and (b) not disclose Customer Data, except as required by law or expressly allowed. Neither party will make any public statement about this agreement's terms without the other's prior written consent.

Term, Termination, and Suspension.

Term and termination. This agreement will remain in effect for three years subject to each party's right under the Master Agreement and applicable law to terminate for convenience. It may be extended, based upon the mutual consent of the parties, during the term of the Master Agreement.

Customer Data. Purchasing Entity may extract Customer Data at any time. If Purchasing Entity's Subscription expires or terminates, Contractor and Microsoft will keep your Customer Data in a limited account for at least 90 days so Purchasing Entity may extract it. Contractor and Microsoft may delete Purchasing Entity's Customer Data after that, and specifically with regard to DPT Services will delete Purchasing Entity's Customer Data after no more than 180 days.

Regulatory. If a government rule or regulation applies to Contractor or Microsoft, but not generally to other businesses, and makes it difficult to operate In-Scope Services without change, or Contractor or Microsoft believe this agreement or an In-Scope Service may conflict with the rule or regulation, Microsoft may change the applicable In-Scope Service(s) or Contractor may terminate the agreement. If Microsoft changes In-Scope Services to come into compliance, and Purchasing Entity does not like the change, Purchasing Entity may terminate.

Suspension. Microsoft may suspend use of In-Scope Services: (1) if reasonably needed to prevent unauthorized Customer Data access; (2) if Purchasing Entity does not promptly respond under §5 to intellectual property claims; (3) for non-payment; or (4) if Purchasing Entity violates the AUP. A suspension will be in effect only while the condition or need exists and, if under clause (1) or (2), will apply to the minimum extent necessary. Contractor or Microsoft will notify Purchasing Entity before suspension, unless doing so may increase damages. Contractor will notify Purchasing Entity at least 30 days before suspending for non-payment. If Purchasing Entity does not fully address the reasons for suspension within 60 days after suspension, Contractor may terminate Purchasing Entity's Subscription.

Limited warranty; disclaimer.

Contractor warrants that In-Scope Services will meet the SLA terms during the Subscription; Purchasing Entity's only remedy for breach of warranty is stated in the SLA. *Contractor provides no (and disclaims to the extent permitted by law any) other warranties, express, implied, or statutory, including warranties of merchantability or fitness for a particular purpose.*

Indemnification.

a. Subject to the exceptions below and the NASPO Participants' (as defined below) compliance with the notice and defense provisions below, in the event of any defect or deficiency in any Microsoft Products or Services purchased by a Participating Entity or Purchasing Entity, Microsoft agrees to defend NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees (collectively, the "NASPO Participants") against third party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property suffered by such third party and caused by the negligence, or willful misconduct of Microsoft, its employees or subcontractors or volunteers, at any tier, during the performance of this Master Agreement (a "PI Claim"). This clause shall not be construed to bar any legal remedies Microsoft may have with respect to the NASPO Participants' failure to fulfill their obligations pursuant to the Master Agreement or any Participating Addendum.

To qualify for such defense, the Participating Entities/Purchasing Entities shall promptly notify Microsoft of any PI Claim of which the Participating Entities/Purchasing Entities become aware which may give rise to a right of defense pursuant to this Section. Notice of any PI Claim that is a legal proceeding, by suit or otherwise, must be provided to Microsoft within thirty (30) days of the Participating Entities'/Purchasing Entities' first learning of such proceeding. If the Participating Entity's/Purchasing Entity's laws require approval of a third party to defend Participating Entity/Purchasing Entity, Participating Entity/Purchasing Entity will seek such approval and if approval is not received, Microsoft is not required to defend that Participating Entity/Purchasing Entity. If a PI Claim is settled, to the extent permitted by law, the Participating Entities/Purchasing Entities shall not publicize the settlement and will cooperate with Microsoft so that Microsoft can make every effort to ensure the settlement agreement contains a non-disclosure provision.

Notwithstanding anything to the contrary contained herein, Participating Entities/Purchasing Entities agree that Microsoft has no obligation for any PI Claim covered by this Section arising out of or resulting from the Participating Entities'/Purchasing Entities' or any of their respective employees', contractors' or agents' acts of negligence, gross negligence or misconduct. THE FOREGOING SHALL CONSTITUTE EACH AND EVERY PARTICIPATING ENTITY'S/PURCHASING ENTITY'S SOLE REMEDY AND MICROSOFT'S SOLE AND EXCLUSIVE LIABILITY FOR ALL PI CLAIMS.

b. **Indemnification** – Intellectual Property. Subject to the NASPO Participant's compliance with the notice and defense requirements and exceptions set forth below, Microsoft agrees to defend the NASPO Participants against any claims made by an unaffiliated third party that any Product or Service or its proper or reasonably expected or acceptable use infringes that third party's patent, copyright, or trademark or makes unlawful use of its trade secret (an "Intellectual Property Claim").

(1) Microsoft's obligations under this section shall not extend to any claims based on:

(a) Microsoft's compliance with a Participating Entity's/Purchasing Entity's designs, specifications or instructions; or

(b) Microsoft's use of technical information or technology provided by the Participating Entity/Purchasing Entity; or

(c) Non-Microsoft software, modifications a Participating Entity/Purchasing Entity makes to, or any specifications or materials a Participating Entity/Purchasing Entity provides or makes available for, a Product; or

(d) Participating Entity's/Purchasing Entity's combination of the Product or Service with a Non-Microsoft product, data or business process; or damages based on the use of a Non-Microsoft product, data or business process; or

(e) Participating Entity's/Purchasing Entity's use of either Microsoft's trademarks or the use or redistribution of a Product or Service in violation of this Master Agreement, Participating Addendum, or any other agreement incorporating its terms; or

(f) Participating Entity's/Purchasing Entity's use of a Product or Service after Microsoft notifies Participating Entity/Purchasing Entity to discontinue that use due to a third party claim.

(2) To qualify for such defense, the involved NASPO Participants (the "Indemnified Party") shall promptly notify Microsoft of any Intellectual Property Claim of which the Indemnified Party become aware which may give rise to right of defense pursuant to this Section. Notice of any Intellectual Property Claim that is a legal proceeding, by suit or otherwise, must be provided to Microsoft within thirty (30) days of the Indemnified Party's learning of such proceeding. If the Indemnified Party's laws require approval of a third party to defend the Indemnified Party, the Indemnified Party will seek such approval and if approval is not received, Microsoft is not required to defend that Indemnified Party. In the event the Indemnified Party does not authorize sole control to Microsoft over any claims that may arise under this subsection, then the parties agree that Microsoft will be granted authorization to equally participate in any proceeding subject to this subsection. 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 Microsoft's reasonable request and expense, information and assistance necessary for such defense. If Microsoft 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 Microsoft 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.

If Microsoft reasonably believes that a Product or Service may infringe or misappropriate a third-party's intellectual property rights, Microsoft will seek to:

i. procure for Participating Entities/Purchasing Entities the right to continue to use the Product or Service; or

ii. modify or replace it with a functional equivalent to make it non-infringing and notify Participating Entities/Purchasing Entities to discontinue use of the prior version, which Participating Entities/Purchasing Entities must do immediately.

If the foregoing options are not commercially reasonable for Microsoft, or if required by a valid judicial or government order, Microsoft may cause Contractor to terminate Participating Entities'/Purchasing Entities' license or access rights in the Product or Service. In such a case, Microsoft will provide Participating Entities/Purchasing Entities with notice and refund any amounts Participating Entities/Purchasing Entities have paid for those rights to the Product or Service.

THE FOREGOING SHALL CONSTITUTE THE LEAD STATE'S AND EACH AND EVERY PARTICIPATING AND/OR PURCHASING ENTITIES' SOLE REMEDY AND MICROSOFT'S SOLE AND EXCLUSIVE LIABILITY FOR ALL INTELLECTUAL PROPERTY CLAIMS.

Limitation of Liability.

The parties agree that, other than In-Scope Services, no other Microsoft Products shall be purchased hereunder. As applicable to In-Scope Services, the following terms and conditions shall apply:

a. General. The total liability of each party for In-Scope Services hereunder (Microsoft, Contractor and each Purchasing Entity, including their Affiliates and contractors), for claims arising under this Agreement, is limited to direct damages up to the amount Purchasing Entity paid for the In-Scope Service during the prior 12 months before the cause of action arose; but in no event will a party's aggregate liability for any In-Scope Service exceed the total amount paid for that In-Scope Service under this Agreement. In the case of In-Scope Services provided free of charge, previews, or code that a Purchasing Entity is authorized to redistribute to third parties without separate payment to Contractor, Microsoft's liability is limited to direct damages up to U.S. $5,000. These limitations apply regardless of whether the liability is based on breach of contract, tort (including negligence), strict liability, breach of warranties, or any other legal theory.

b. Affiliates and contractors. Contractor and Purchasing Entity each agree not to bring any action against the other's Affiliates or contractors in respect of any matter disclaimed on their behalf in this Agreement. Each party will be responsible for its actions in the event of any breach of this provision.

c. EXCLUSION OF CERTAIN DAMAGES. Neither party nor their Affiliates or contractors will be liable for any indirect, consequential, special or incidental damages, or damages for lost profits, revenues, business interruption, or loss of business information in connection with this agreement, even if advised of the possibility of such damages or if such possibility was reasonably foreseeable.

d. Limits. *The limits and exclusions in this section titled "Limitation of liability" do not apply to either party's (1) obligations under the section titled "Defense of third party claims", (2) liability for damages caused by either party's gross negligence or willful misconduct, or that of its employees or its agents, and awarded by a court of final adjudication (provided that, in jurisdictions that do not recognize a legal distinction between "gross negligence" and "negligence," "gross negligence" as used in this subsection shall mean "recklessness"); and (3) liability for violation of its confidentiality obligations (except obligations related to Customer Data) or the other party's intellectual property rights.*

Agreement mechanics

Purchasing Entity must send notice by regular mail, return receipt requested, to the address on the Portal (effective when delivered). Contractor or Microsoft may email notice to your account administrators (effective when sent). Purchasing Entity may not assign this agreement, or any right or duty under it. If part of this agreement is held unenforceable, the rest remains in force. Failure to enforce this agreement is not a waiver. The parties are independent contractors. This agreement does not create an agency, partnership, or joint venture. This agreement is governed by the laws applicable to Purchasing Entity, without regard to conflict of laws. This agreement (including the SLA and OST) and Contractor's price sheet are the parties' entire agreement on this subject and supersedes any concurrent or prior communications. Agreement terms that require performance, or apply to events that may occur, after termination or expiration will survive, including §5. In-Scope Service and any Client associated therewith are subject to U.S. export jurisdiction. Purchasing Entity must comply with the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end-use, and destination restrictions. For more information, see http://www.microsoft.com/exporting/. Microsoft delivers In-Scope Services, and the rights granted to us also apply to them.

Miscellaneous Microsoft Terms and Conditions

Accessibility. Microsoft supports the government's obligation to provide accessible technologies to its citizens with disabilities as required by Section 508 of the Rehabilitation Act of 1973, and its state law counterparts (including applicable California provisions). Microsoft encourages its customers (including Purchasing Entities under the Master Agreement and Participating Addenda) to judiciously compare product accessibility performance. The Voluntary Product Accessibility Templates ("VPATs") for the Microsoft technologies used in providing the online services can be found at Microsoft's VPAT page. Further information regarding Microsoft's commitment to accessibility can be found at www.microsoft.com/enable.

DPT Services Information Security Policy. For each DPT Service, Microsoft follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

DPT Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Dynamics CRM Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes

**Does not include Yammer Enterprise.*

***Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.*

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above, unless it is no longer used in the industry and it is replaced with a successor (if any). Azure Government Services meet a separate set of control standards and frameworks, as detailed on the Microsoft Azure Trust Center.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Purchasing Entity, along with other information reasonably requested by Purchasing Entity regarding Microsoft security practices and policies.

Purchasing Entity is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Purchasing Entity's requirements.

Microsoft Audits of DPT Services. For each DPT Service, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each DPT Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Microsoft's Confidential Information. The Microsoft Audit Report will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If Purchasing Entity requests, Microsoft will provide Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Microsoft's compliance with the security obligations under the DPT. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

HIPAA/HITECH Business Associate. If Purchasing Entity is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data, as those terms are defined in 45 CFR § 160.103, this agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the DPT Services to which it applies and is available at http://aka.ms/BAA. Purchasing Entity may opt out of the BAA by instructing Contractor to send the following information to Microsoft in a written notice (under the terms of the Contractor's subcontract with Microsoft):

- the full legal name of Purchasing Entity and any Affiliate that is opting out;
- the volume licensing agreement number to which the opt out applies.

FedRAMP. During the term of a Purchasing Entity's subscription for Government Community Cloud Services, those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level. Microsoft intends for Government Community Cloud Services to support FedRAMP Authority to Operate ("ATO"), and Microsoft will use commercially reasonable efforts to obtain an ATO from a Federal agency, and to maintain such ATO through continuous monitoring processes and by conducting regular FedRAMP audits.

Background Checks. Microsoft performs the following background checks on all US personnel who have potential to access Customer Data. Adherence to this policy is one of the control procedures addressed by the Microsoft Audit Report per the section of the Microsoft Online Services Terms titled "Microsoft Audits of Online Services." Such Background Checks will be performed in accordance with the Fair Credit Reporting Act and will consist of Social Security Number trace, seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes, Office of Foreign Assets Control List (OFAC) check, Bureau of Industry and Security List (BIS) check and Office of Defense Trade Controls Debarred Persons List (DDTC) check.

Additionally, for States with which Microsoft has entered into a Microsoft CJIS Information Agreement and provided an FBI CJIS Addendum Certification to the applicable CJIS Systems Agency (CSA, e.g. the California Department of Justice), for its CJIS Covered Services (which are most of the Microsoft Government Community Cloud Services), Microsoft submits its personnel that have access to unencrypted Criminal Justice Information and other Customer Content (including both employees and subcontractors, where applicable) for FBI NCIC fingerprint background checks and adjudication by each such CSA.

Click-Through Terms. For the Microsoft In-Scope Services sold and licensed to Purchasing Entities hereunder, no click-through licensing terms presented to end users or administrators, as they pertain to the delivery, operation or use of such services, shall be binding. For clarity, to the extent that certain services may present terms of use for a web portal used to administer and configure the In-Scope Services, or to download software in conjunction with the In-Scope Services, such terms of use shall be binding, to the extent that there are no equivalent terms and conditions in the Master Agreement which pertain to the use of such web portals.

Definitions.

"AUP" means the section of the OST titled "Acceptable Use Policy""Azure Consumption-Based Services" means any Microsoft Online Service made available for Purchasing Entity's use and consumption under the Microsoft Azure Administrative Portal, following Purchasing Entity's initial subscription order for such services, subject to consumption fees billed to Purchasing Entity (or debited against its prepaid Azure monetary commitment balance, if applicable) as described in the applicable Product Terms.

"Client" means device software, if any, that Contractor or Microsoft provides to Purchasing Entity with In-Scope Services.

"Customer Content" means the subset of Customer Data created by users, which includes the following:

- For Office 365 Services, Customer Content shall at least include Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content and the files stored within that site, and Skype for Business Online archived conversations.
- For Microsoft Dynamics CRM Online Services, Customer Content means the entities of Customer Data managed by the Microsoft Dynamics CRM Online Services.
- For Microsoft Azure Core Services, Customer Content includes all Customer Data except as may be noted in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but will not add exceptions for existing Microsoft Azure Core Services in general release).
- For Microsoft Intune Online Services, Customer Content includes all Customer Data except as may be noted in the "Data Location" section of the Microsoft Intune Trust Center.

“Customer Data” means all data, including all text, sound, or image files that are provided to Microsoft by, or on behalf of, Purchasing Entity through its use of In-Scope Services.

“DPT” means the section of the OST titled “Data Processing Terms.”

“DPT Services” means the Microsoft Online Services to which the DPT applies. As of the date this agreement was executed by the parties, DPT Services include “Microsoft Dynamics CRM Online Services,” “Office 365 Services,” “Microsoft Intune Online Services,” and “Microsoft Azure Core Services,” which consist of the following component Microsoft Online Services:

DPT Services	
Microsoft Dynamics CRM Online Services	Microsoft Dynamics CRM Online services made available through volume licensing or the Microsoft online services portal, excluding (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones and (2) any separately-branded service made available with or connected to Microsoft Dynamics CRM Online, such as Microsoft Social Engagement, Parature, from Microsoft, and Microsoft Dynamics Marketing.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft’s control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded “for Office 365.”
Microsoft Azure Core Services	Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Batch, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Notification Hub, Workflow Manager, Express Route, Scheduler, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, and HDInsight.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.

“Government Community Cloud Services” means the Microsoft Online Services identified as such (a subset of DPT Services) in the DPT and Product Terms.

“In-Scope Services” means the Microsoft Online Services for which subscription licenses are sold to Purchasing Entity by Contractor. In-Scope Services include, but are not limited to DPT Services. Except for Azure Consumption-Based Services (which are billed based upon the quantities of such services consumed by Purchasing Entity), Purchasing Entity will order individual licenses from Contractor for all In-Scope Services Licenses.

“Master Agreement” means the agreement (described therein as “NASPO ValuePoint Master Agreement for Cloud Services”) between Contractor and the Lead State, subject to the terms and conditions of the Participating Addendum between Contractor and Purchasing Entity’s State (if different from Utah), and which resulted from award of contract under Utah Solicitation Number CH16012.

“Microsoft” means Microsoft Corporation, which is subcontractor to Contractor and delivers the In-Scope Services.

“Online Services” means the Microsoft-hosted services for which Purchasing Entity acquires Licenses from Contractor hereunder.

“OST” means the Microsoft “Online Services Terms,” which are additional terms that apply to Purchasing Entity’s use of Online Services published on the Volume Licensing Site and updated from time to time, and is subject to terms and conditions in the OST which govern which version of OST is applicable to a particular subscription order.

"Portal" means the Online Services Portal for each In-Scope Service.

"Product Terms" means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is available on the Volume Licensing Site and is updated from time to time.

"Security Incident" means any unlawful access, use, theft or destruction to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in use, theft, loss, disclosure, alteration or destruction of Customer Data. All references to "Data Breach" in the Master Agreement shall be deemed to mean Security Incident.

"Service Level Agreement" ("SLA") means the document which specifies the standards to which Microsoft agrees to adhere and by which it measures the level of service for an In-Scope Service. Microsoft's current and archived prior version SLAs are available at the Volume Licensing Site. With respect to any In-Scope Service ordered under the this Agreement, the most current SLA available at the onset of a subscription License term shall apply to that In-Scope Service for the duration of that subscription License Term, after which (for any subsequent renewal subscription License term) it will be superseded by the version current at the time of renewal.

"Subscription" means an order for a quantity of an In-Scope Service, including but not limited to (a) orders for User Subscription Licenses for one or more In-Scope Services; and (b) an order for the purpose of establishing a subscription for Azure Consumption-Based Services.

"Volume Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.

ATTACHMENT E-2

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.

e. At no time shall any Customer Data — 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.

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.

9. Access to Security Logs and Reports: Solely for DPT Services, the section of the DPT titled “Event Logging” shall apply. For clarity, Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Microsoft shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity’s Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change. **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, and provide service to customers as defined in the SLA.

17. Subcontractor19. Business Continuity and Disaster Recovery: Solely for DPT Services, the following terms and conditions shall apply:

Part 1: Data retention:

Customer Data will be processed and retained intact for the duration of Customer’s subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Microsoft has specific procedures in place governing access to copies of Customer Data.

- Microsoft reviews data recovery procedures at least every six months.

- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Microsoft will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Microsoft shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Microsoft customers and their data, or would compromise the security of the DPT Services, will be withheld. For clarity, “data restoration efforts” does not include automated Customer Data recovery processes such as when one of Microsoft’s datacenters is activated upon failure of another.

21. Web Services: Where applicable, 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: To whatever extent a form or use of encryption is required of Microsoft pursuant to any of the industry and Federal government standards committed by Microsoft in this Master Agreement and the Microsoft Online Services Terms, Microsoft will comply with such requirements.

PLATFORM AS A SERVICE

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

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

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

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

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

e. At no time shall any Customer Data — 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.

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.

9. Access to Security Logs and Reports: Solely for DPT Services, the section of the DPT titled "Event Logging" shall apply. For clarity, Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Microsoft shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

18. Business Continuity and Disaster Recovery: Solely for DPT Services, the following terms and conditions shall apply:

Part 1: Data retention:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Microsoft has specific procedures in place governing access to copies of Customer Data.

- Microsoft reviews data recovery procedures at least every six months.

- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Microsoft will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Microsoft shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Microsoft customers and their data, or would compromise the security of the DPT Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Microsoft's datacenters is activated upon failure of another.**20. Web Services:** Where applicable, the Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: To whatever extent a form or use of encryption is required of Microsoft pursuant to any of the industry and Federal government standards committed by Microsoft in this Master Agreement and the Microsoft Online Services Terms, Microsoft will comply with such requirements.

INFRASTRUCTURE AS A SERVICE

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

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

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

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

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

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

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

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

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

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.

9. Access to Security Logs and Reports: Solely for DPT Services, the section of the DPT titled "Event Logging" shall apply. For clarity, Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Microsoft shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

18. Business Continuity and Disaster Recovery: Solely for DPT Services, the following terms and conditions shall apply:

Part 1: Data retention:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Microsoft has specific procedures in place governing access to copies of Customer Data.

- Microsoft reviews data recovery procedures at least every six months.

- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Microsoft will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Microsoft shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Microsoft customers and their data, or would compromise the security of the DPT Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Microsoft's datacenters is activated upon failure of another.

ATTACHMENT E-3

AWS PUBLIC SECTOR ACCESS POLICY

https://s3.amazonaws.com/Reseller-Program-Legal-Documents/AWS+Access+Policy.pdf

ATTACHMENT E-4

CA TERMS AND CONDITIONS - Placeholder